Deutscher Bundestag **Drucksache 17/8500**
17. Wahlperiode 26. 01. 2012

Unterrichtung

durch die Bundesregierung

Rahmenprogramm der Bundesregierung „Forschung für die zivile Sicherheit (2012 bis 2017)“

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums für Bildung und Forschung vom 25. Januar 2012.

Zusammenfassung

Die Globalisierung eröffnet Deutschland als moderner Industrie- und Wissensgesellschaft vielfältige Zukunftschancen. Mit ihr sind aber auch neue Herausforderungen verbunden, denen wir uns in Gesellschaft, Wirtschaft und Politik stellen müssen. Die Vernetzung internationaler Handels- und Reiseströme, die Allverfügbarkeit des Internets ebenso wie die von Extremwetterereignissen ausgehenden Schadenspotenziale oder die Bedrohung eines weltweit operierenden Terrorismus haben zu neuen Verwundbarkeiten geführt. Verwundbarkeiten, vor denen wir uns in unserer gleichermaßen weltoffenen wie hoch technisierten Zivilgesellschaft schützen müssen.

Sicherheit ist die Basis eines freien Lebens und ein wichtiger Faktor des wirtschaftlichen Wohlstandes in Deutschland. Wenn wir auch in Zukunft die individuelle Freiheit, die Unversehrtheit aller Bürgerinnen und Bürger und lebenswichtige staatliche und wirtschaftliche Infrastrukturen wirksam schützen wollen, müssen wir nach neuen Wegen und Lösungen suchen. Es gilt, aufbauend auf den Erfolgen des ersten nationalen Forschungsprogramms „Forschung für die zivile Sicherheit", die Stärken der zivilen Sicherheitsforschung für die Entwicklung innovativer Lösungen zu nutzen und dazu beizutragen, eine ausgewogene Balance zwischen Freiheit und Sicherheit zu bewahren.

Im Mittelpunkt stehen Lösungen, die den Schutz der Bevölkerung und der kritischen Infrastrukturen vor Bedrohungen durch Terrorismus, Sabotage, organisierte Kriminalität, Piraterie, aber auch vor den Folgen von Naturkatastrophen und Großunfällen gewährleisten und einen Beitrag zum Schutz unseres freiheitlichen Lebensstils leisten.

Mit dem Rahmenprogramm „Forschung für die zivile Sicherheit" investiert die Bundesregierung in die Sicherheit von morgen. Das Rahmenprogramm setzt damit die Impulse der „Hightech-Strategie 2020 für Deutschland" um, in der Sicherheit eines von fünf Bedarfsfeldern ist, an denen sich die innovationspolitischen Aktivitäten der Bundesregierung orientieren.

Das Rahmenprogramm richtet seine Forschungsförderung auf die globalen Herausforderungen der zivilen Sicherheit aus:

Sicherheit kritischer Infrastrukturen: Die Sicherheitsarchitektur Deutschlands befindet sich im Wandel. Um das hohe Sicherheitsniveau in Deutschland auch in Zukunft zu erhalten und auszubauen, werden wir die Forschung darauf ausrichten, neue Verwundbarkeiten möglichst frühzeitig zu erkennen und die Robustheit kritischer Infrastrukturen durch Innovationen kontinuierlich zu erhöhen.

Sicherheit der Wirtschaft: Unternehmen aus Deutschland sind in einer modernen Industriegesellschaft und im globalen Wettbewerb verstärkt Risiken ausgesetzt. Durch Forschung und Innovationen wollen wir insbesondere mittelständische Unternehmen und Betreiber kritischer Infrastrukturen dazu befähigen, ihre technologischen Kernkompetenzen und ihr Know-how besser vor natürlichen Risiken und organisierter Wirtschaftskriminalität zu schützen.

Sicherheit im Cyberraum: Die Sicherheit kritischer Informationsinfrastrukturen ebenso wie die Gewährleistung einer permanenten Verfügbarkeit des Cyberraums stellen eine der großen gemeinsamen Herausforderungen für Staat, Wirtschaft und Gesellschaft im 21. Jahrhundert dar. Im Fokus der Forschung stehen Lösungen, die den Schutz des Cyberraums vor schwerwiegenden Angriffen kontinuierlich und unter Wahrung des Schutzes persönlicher Daten und der Privatsphäre verbessern.

Sicherheit der Bürgerinnen und Bürger: Sicherheitsforschung wird an gesellschaftlichen Fragestellungen ausgerichtet, die Bürgerinnen und Bürger in ihrem unmittelbaren Lebensumfeld betreffen. Wir wollen durch gezielte Forschung einen Beitrag dazu leisten, den Schutz der Bevölkerung und ihrer Lebensgrundlagen sicherzustellen und einen breiten gesellschaftlichen Dialog zur Ausgestaltung der zivilen Sicherheit in Deutschland anstoßen.

Das Rahmenprogramm „Forschung für die zivile Sicherheit" verfolgt einen ganzheitlichen, integrierten Forschungsansatz, der die gesamte Innovationskette von der Forschung bis zur Anwendung einbezieht. Dabei orientieren wir uns am Bedarf der Endnutzer – also insbesondere der Behörden und Organisationen mit Sicherheitsaufgaben sowie der Betreiber kritischer Infrastrukturen. Über Disziplingrenzen hinweg greifen alle relevanten Akteure aus Wissenschaft, Wirtschaft und Staat in den Forschungsschwerpunkten konkrete Fragestellungen auf und arbeiten gemeinsam an der Entwicklung innovativer und wettbewerbsfähiger Produkte und Dienstleistungen. Dabei steht immer die Frage im Vordergrund, wie Forschung und der Einsatz neuer Sicherheitslösungen dazu beitragen können, die zivile Sicherheit der Menschen zu erhöhen, ohne den Schutz bürgerlicher Grundwerte wie Freiheit und Selbstbestimmung zu beeinträchtigen. Ziel des Rahmenprogramms ist es, die wirtschaftlichen Chancen der zivilen Sicherheitsforschung zu nutzen und Deutschland als führenden Anbieter von Sicherheitstechnologien zu etablieren.

Innovationstransfer unterstützen

Die Umsetzung innovativer Sicherheitslösungen in die Praxis kann nur gelingen, wenn sie sich sowohl in der Gesellschaft, im alltäglichen Einsatz als auch am Markt bewähren. Wir werden deshalb die Sicherheitsforschung und Maßnahmen des Innovationstransfers konsequent miteinander verzahnen, um die internationale Vorreiterstellung deutscher Anbieter ziviler Sicherheitsprodukte und -technologien langfristig auszubauen.

Wissenschaftliche Basis verbreitern und Kompetenzbildung unterstützen

Als international anerkannter Wissenschafts- und Innovationsstandort muss sich Deutschland den Herausforderungen des globalen Wettbewerbs auch im Bereich von Forschung, Lehre und Ausbildung stellen. Wir wollen die

interdisziplinäre und interinstitutionelle Zusammenarbeit in der zivilen Sicherheitsforschung stärken und die Weiterentwicklung interdisziplinärer akademischer Ausbildungsstrukturen und -angebote fördern.

Der richtige Umgang mit Risiken und konkreten Gefahrensituationen ist keine Selbstverständlichkeit. Er erfordert umfangreiche Kompetenzen und die Fähigkeit, erworbenes Wissen in Alltagssituationen, im Berufsleben oder bei ehrenamtlichen Tätigkeiten schnell und effektiv einzusetzen. Wir wollen uns dafür einsetzen, die technischen und organisatorischen Kompetenzen von Sicherheits- und Rettungskräften oder von Mitarbeiterinnen und Mitarbeitern in Unternehmen zu verbessern und den Aufbau individueller Sicherheitskompetenzen in der Bevölkerung unterstützen.

Internationale Zusammenarbeit stärken

Deutschland strebt auf dem Gebiet der zivilen Sicherheitsforschung eine aktive Rolle an, um die Entwicklung von Lösungsansätzen für globale Herausforderungen mitzugestalten. Wir werden die bestehenden Forschungsallianzen mit starken internationalen Technologiepartnern ausbauen, um weltweit verfügbares Wissen und Knowhow für das nationale Programm nutzbar zu machen. Darüber hinaus streben wir gezielte bilaterale Forschungskooperationen mit Staaten an, die sich zu wichtigen Wachstumsmärkten der zivilen Sicherheit entwickeln werden.

1 Sicherheit als Basis eines freien Lebens

Die Herausforderungen für die Sicherheit in einer modernen Industrie- und Wissensgesellschaft haben sich grundlegend gewandelt. Mit der weiter fortschreitenden Globalisierung von Gesellschaft, Wirtschaft und Politik eröffnen sich für Deutschland neue Chancen. Als weltoffene Gesellschaft und exportorientierte Wirtschaftsnation profitieren wir in hohem Maße von der zunehmenden Vernetzung internationaler Handels-, Reise- und Wissensströme.

Dadurch entstehen aber auch neue Verwundbarkeiten. Diese können sich auf die äußere und innere Sicherheit Deutschlands ebenso auswirken wie auf die individuelle Freiheit und Unversehrtheit seiner Bürgerinnen und Bürger.

Sicherheit als Chance für die Zukunft

Sicherheit ist ein wichtiger Standort- und Wirtschaftsfaktor. Wir profitieren von unserem hohen Sicherheitsniveau zum Beispiel bei den Liefer- und Warenketten, der Energieversorgung sowie den Informations- und Verkehrsinfrastrukturen.

Leistungsfähige Hightech-Lösungen und innovative Dienstleistungen werden dazu beitragen, dieses hohe Niveau zu halten. Gleichzeitig eröffnen sie die Chance, Deutschland zu einem Leitmarkt für Sicherheitslösungen zu machen.

Forschung für die zivile Sicherheit

Wir müssen neue Wege suchen, um unsere Freiheit und Rechtsstaatlichkeit zu sichern. Dabei sind Sicherheit und Freiheit kein Gegensatz. Sie stehen aber in einem Spannungsverhältnis. Zu wenig Sicherheit bedroht unseren freiheitlichen Lebensstil. Zu viel Sicherheit kann unsere persönliche Freiheit und das Recht auf informationelle Selbstbestimmung gefährden. Sicherheitsforschung, wie wir sie verstehen, hat dieses Spannungsfeld immer im Blick. Sie wird dazu beitragen, eine ausgewogene Balance zwischen Freiheit und Sicherheit zu bewahren.

Mit dem Rahmenprogramm „Forschung für die zivile Sicherheit“ investiert die Bundesregierung in die Sicherheit von morgen. Im Einklang mit der „Hightech-Strategie 2020 für Deutschland“ verfolgen wir einen ganzheitlichen, integrierten Forschungsansatz, der die gesamte Innovationskette von der Forschung bis zur Anwendung einbezieht. Dies erfordert vernetztes Denken und Handeln, bei dem unterschiedlichste Akteure aus Wissenschaft, Wirtschaft und Staat über Disziplingrenzen hinweg gemeinsam Lösungen für konkrete Bedrohungsszenarien entwickeln.

Sicherheit ist ein Querschnittsthema

Technologien, die im Rahmen der zivilen Sicherheitsforschung entwickelt wurden, können auch in anderen Bereichen, wie zum Beispiel der Anlagensicherheit, zu Lösungen beitragen. Um eine hohe Effizienz in der Forschung zu erreichen, soll der Austausch von Wissen zwischen verschiedenen Bereichen unterstützt werden. Die Differenzierung entsteht dort, wo Forschung auf konkrete Anwendungen ausgerichtet wird.

Auf Erfolgen aufbauen

Anfang 2007 haben wir erstmals ein nationales Forschungsprogramm zur zivilen Sicherheit gestartet. Seitdem hat sich die zivile Sicherheitsforschung in Deutschland als eigenständiges Forschungsgebiet mit einer gut vernetzten Akteurslandschaft etabliert. Das stärkt die Position deutscher Akteure im internationalen Wettbewerb und eröffnet vielfältige Chancen, die Zusammenarbeit im Rahmen der Europäischen Union und den Ausbau internationaler Forschungsallianzen mit ausgewählten Partnern zu forcieren.

Mit der Fortschreibung des Forschungsprogramms knüpfen wir an die erreichten Erfolge an. Die Forschungsschwerpunkte werden auf die künftigen Herausforderungen der zivilen Sicherheit ausgerichtet.

Ausrichtung auf die Herausforderungen

Im Rahmen der zivilen Sicherheitsforschung werden zukünftige Risiken für unsere Gesellschaft systematisch analysiert und innovative, wettbewerbsfähige Produkte und Dienstleistungen entwickelt. Im Mittelpunkt stehen Lösungen, die den Schutz der Bevölkerung und der kritischen Infrastrukturen vor Bedrohungen durch Terrorismus, Sabotage, organisierte Kriminalität, Piraterie, aber

auch vor den Folgen von Naturkatastrophen und Großunfällen gewährleisten können.

Unsere Forschungsförderung adressiert die globalen Herausforderungen der zivilen Sicherheit:

Sicherheit kritischer Infrastrukturen: Die Sicherheitsarchitektur Deutschlands befindet sich im Wandel. Nicht zuletzt durch das Aufkommen eines international vernetzten Terrorismus muss sich Deutschland einem veränderten Sicherheitsumfeld stellen. Gleichzeitig hat die zunehmende Vernetzung der Infrastrukturen zur Folge, dass bereits kleine Störungen in einem Bereich zu weitreichenden Ausfällen auch in anderen Infrastrukturen führen können.

Unsere Aufgabe ist es, die Sicherheit und Robustheit kritischer Infrastrukturen durch Forschung und Innovation kontinuierlich zu erhöhen.

Sicherheit der Wirtschaft: Unternehmen aus Deutschland sind in einer modernen, arbeitsteiligen Industriegesellschaft und im globalen Wettbewerb verstärkt Risiken ausgesetzt. Diese Risiken schließen nicht nur Industrieanlagen und Menschen ein, sondern auch alle Unternehmensprozesse – von der Rohstoffversorgung über die Produktion bis hin zum Vertrieb.

Der Schutz des Produktionsfaktors Wissen wird immer bedeutsamer. Bereits heute führen die internationalen Unternehmens- und Informationsverflechtungen dazu, dass informationelle Angriffe bzw. Industriespionage hohe wirtschaftliche Schäden insbesondere in mittelständischen Unternehmen verursachen.

Sicherheit im Cyberraum: Die Verfügbarkeit des Cyberraums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind zu einer existenziellen Frage des 21. Jahrhunderts geworden. Staat, kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen.

Fehlerbehaftete IT-Produkte und -komponenten, der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyberraum können zu erheblichen Beeinträchtigungen führen. Die Gewährleistung der Sicherheit im Cyberraum wird damit zur zentralen gemeinsamen Herausforderung für Staat, Wirtschaft und Gesellschaft.

Sicherheit der Bürgerinnen und Bürger: Sicherheitsforschung wird an gesellschaftlichen Fragestellungen ausgerichtet, die Bürgerinnen und Bürger in ihrem unmittelbaren Lebensumfeld betreffen. Das schließt einen besseren Schutz im öffentlichen Personennahverkehr vor kriminellen Übergriffen ebenso ein wie präventive Maßnahmen zur Stärkung der Selbsthilfefähigkeit der Bevölkerung in Katastrophenfällen.

Dabei steht immer die Frage im Vordergrund, wie Forschung und der Einsatz neuer Sicherheitslösungen dazu beitragen können, die zivile Sicherheit der Menschen zu erhöhen, ohne den Schutz bürgerlicher Grundwerte wie Freiheit und Selbstbestimmung zu beeinträchtigen.

Ziele des Rahmenprogramms

- Wir werden mit der Sicherheitsforschung einen Beitrag zum Schutz unseres freiheitlichen Lebensstils leisten
- Wir werden datenschutzrechtliche Belange aufgreifen und die Entwicklung datenschutzfreundlicher Lösungen fördern
- Wir wollen einen breiten gesellschaftlichen Dialog zur Ausgestaltung von ziviler Sicherheit in Deutschland anstoßen
- Wir werden die zivile Sicherheitsforschung an aktuellen und künftigen Herausforderungen ausrichten und die Entwicklung innovativer Lösungen für den Schutz der Bevölkerung und der kritischen Infrastrukturen fördern
- Wir werden Sicherheitsforschung auf den gesamten Resilienzzyklus (Krisenprävention, Vorsorge, Krisenreaktion sowie Wiederherstellung und Auswertung) ausrichten
- Wir werden uns am Bedarf der Endnutzer – also der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sowie der Betreiber kritischer Infrastrukturen – orientieren und die gesamte Innovationskette von der Forschung über die Industrie bis hin zu den Endnutzern einbeziehen
- Wir wollen die wirtschaftlichen Chancen nutzen und Deutschland als führenden Anbieter von Sicherheitstechnologien etablieren
- Wir werden die Sicherheitsforschung und Maßnahmen des Innovationstransfers konsequent miteinander verzahnen
- Wir wollen den Aufbau von Sicherheitskompetenzen in der Gesellschaft unterstützen und die wissenschaftliche Basis verbreitern
- Wir werden internationale Forschungskooperationen ausbauen und die Entwicklung von Lösungsansätzen für globale Herausforderungen mitgestalten

2 Forschungsthemen

2.1 Gesellschaftliche Aspekte der zivilen Sicherheit

Zivile Sicherheit ist grundlegend für das individuelle und soziale Leben aller Bürgerinnen und Bürger. Sie ist nicht zuletzt angesichts der Verwundbarkeiten des modernen Lebens zu einem zentralen Wertbegriff der Gegenwartsgesellschaft geworden und ein wichtiger Faktor des wirtschaftlichen Wohlstands in Deutschland. Zivile Sicherheit ist ein öffentliches Gut, das eng verbunden ist mit gesellschaftlichen Wandlungsprozessen und einem veränderten Freiheitsbegriff, in dem der öffentliche Raum als Raum individueller, kommunikativer und sozialer Freiheit ange-

sehen wird. Das wirkt sich auf die subjektive Wahrnehmung von Sicherheit in der Bevölkerung ebenso aus wie auf die Transformation institutioneller Strukturen und Regelungen zur Gewährleistung von Sicherheit. Zivile Sicherheit steht dabei im Zeichen eines erweiterten Sicherheitsbegriffes. So wird der Schutz der inneren Sicherheit Deutschlands immer mehr von globalen Herausforderungen und dem Wandel staatlicher Vorsorgeaufgaben bestimmt.

Wie stellen wir uns eine sichere Gesellschaft in Zukunft vor? Wie müssen Sicherheitsmaßnahmen gestaltet werden, damit sie die grundrechtliche Freiheitssphäre der Bürgerinnen und Bürger wahren und Bedrohungen verringern? Sind wir bereit, Unsicherheiten zu ertragen? Diese Fragen formulieren eine große Herausforderung an die Sicherheitsforschung. Sowohl die Risiken als auch moderne Sicherheitslösungen sind häufig komplex, mitunter nur schwer begreifbar. Die objektive Sicherheitslage und unser subjektives Sicherheitsempfinden stimmen oft nicht überein. Dabei gilt es auch zu berücksichtigen, dass selbst mehrheitlich in der Bevölkerung akzeptierte Sicherheitslösungen unter ethischen Gesichtspunkten unvertretbar sein können, wenn sie zum Beispiel Minderheiten diskriminieren. Ein gesellschaftlicher Diskurs zu solchen Fragestellungen wird dazu beitragen, Sicherheitslösungen so zu gestalten, dass sie die Bedürfnisse, Bedenken und Erwartungen der Bürgerinnen und Bürger berücksichtigen.

Zivile Sicherheitsforschung kann den Wandel gesellschaftlicher Sicherheitskulturen und institutioneller Sicherheitsarchitekturen erfolgreich mitgestalten. Gefragt sind nicht nur die wissenschaftlich und technisch besten Lösungen, sondern innovative Sicherheitslösungen, die zur Praxis einzelner Organisationen und zur Gesellschaft passen. Deswegen werden von Beginn an alle Akteure in die Forschung eingebunden und technische und gesellschaftliche Fragestellungen verknüpft. Nur so kann es gelingen, proaktiv und unter Einbeziehung rechtlicher, sozialer und ökonomischer Dimensionen die Entwicklung ethisch verantwortbarer Sicherheitstechnologien zu fördern.

Um diesen Herausforderungen zu begegnen, richten wir die Forschung auf folgende Schwerpunkte aus:

Umgang mit Risiken und Quantifizierbarkeit von Sicherheit

Die Risiken für Staat, Wirtschaft und Gesellschaft sind vielschichtiger und unvorhersehbarer geworden. Staatliche wie private Sicherheitsakteure sehen sich einem wachsenden Aufgabenspektrum gegenüber. Grundlage eines wirksamen Schutzes der Bevölkerung und von kritischen Infrastrukturen ist die frühzeitige Identifizierung und Bewertung gesellschaftlicher und technischer Risiken sowie die Quantifizierbarkeit von Sicherheit unter Berücksichtigung sozialer und ökonomischer Kosten.

Forschungsthemen sind unter anderem:

– Entwicklung von Konzepten und Methoden der Risikoanalyse, -bewertung und -priorisierung einschließlich der Bewertung von Restrisiken

– Untersuchungen zum Risikobewusstsein in der Bevölkerung

– Methodik zur Quantifizierung von Sicherheit bzw. zur Evaluierung von technischen und organisatorischen Sicherheitsmaßnahmen

Sicherheitsempfinden und Kriminalität

Die Entwicklung des Sicherheitsempfindens, der Umgang mit Unsicherheit, Angst und Sorge sind Faktoren, welche Bürgerinnen und Bürger in ihrem persönlichen Lebensumfeld berühren und die Gesellschaft und ihr Wertesystem prägen. Das betrifft sowohl den Wandel sicherheitskultureller Werte als auch Veränderungen der persönlichen Wahrnehmung von Sicherheit, die durch den Einsatz moderner Sicherheitstechnik ausgelöst werden können. Vorhandene Erkenntnisse zeigen, dass das subjektive Sicherheitsempfinden der Bevölkerung nicht immer den tatsächlichen Risiken und Bedrohungen, die beispielsweise aus bestimmten Kriminalitätsformen erwachsen, entspricht.

Forschungsthemen sind unter anderem:

– Weiterentwicklung von Methoden zur Kriminalitätskontrolle, -prävention und Wirkungsforschung

– Untersuchungen zu Veränderungen und Einflussfaktoren des Sicherheitsempfindens bzw. der Risikowahrnehmung

– Rolle und Einfluss des Sicherheitsempfindens der Bürgerinnen und Bürgern im Rahmen staatlicher Krisenmanagementkonzepte unter Berücksichtigung einer sich wandelnden Gesellschaftsstruktur

– Schaffung verbesserter Erkenntnisgrundlagen im Bereich der Dunkelfeldforschung und der Rückfallprognose

– dynamische Analyse zukünftiger Bedrohungsentwicklungen und Täterprofile, insbesondere im Bereich der organisierten Kriminalität und der Internetkriminalität

Kommunikation

Der Umgang mit Risiken und eine schnelle und erfolgreiche Krisenbewältigung hängen von der Verfügbarkeit von Informationen und der Effizienz von Kommunikationsprozessen ab. Geeignete Kommunikationsstrategien beziehen alle relevanten Akteure, wie Krisenstäbe, Einsatzkräfte und Veranstalter sowie die Öffentlichkeit ein. Eine akteurs- und zielgruppengerechte Risiko- bzw. Krisenkommunikation nutzt die Möglichkeiten der Neuen Medien und geht auf das sich ändernde Medienverhalten ein. Sie sensibilisiert die Bevölkerung, Risiken und Gefahren frühzeitig wahrzunehmen, und vermittelt Möglichkeiten der Selbsthilfe und Prävention. Gleichzeitig müssen die Kommunikationsprozesse und -kulturen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) so gestaltet sein, dass die Zusammenarbeit zwischen Rettungs- und Einsatzkräften, kommunalen Verantwortungsträgern bzw. Landes- oder Bundesbehörden optimiert wird.

Forschungsthemen sind unter anderem:

- Strategien und Konzepte zu effizienten und interoperablen Kommunikationsstrukturen innerhalb und zwischen Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
- Untersuchungen zu den intendierten und nicht-intendierten Folgen von Kommunikationsinhalten
- Potenziale und Rolle neuer interaktiver Medien (z. B. Internet bzw. Social Media) für die Risiko- und Krisenkommunikation mit der Bevölkerung

Stärkung der Widerstandsfähigkeit (Resilienz)

Zivile Sicherheit kann langfristig nur dann gewährleistet werden, wenn die Widerstandsfähigkeit der Gesellschaft gestärkt wird. Dafür gilt es zum Beispiel, die Robustheit und Sicherheit kritischer Infrastrukturen sowie die Fähigkeit der Bevölkerung zum Überwinden von Krisensituationen zu erhöhen.

Ziel der Forschung ist es, die Widerstandsfähigkeit Deutschlands und damit den Schutz jedes einzelnen Bürgers gegenüber Sicherheitsrisiken und -bedrohungen durch einen systemischen Ansatz zu erhöhen. Forschungsthemen sind unter anderem:

- Entwicklung von Konzepten und analytischen Methoden zur Erhöhung der gesellschaftlichen Resilienz
- Bedarfsanalyse und verbesserte Sensibilisierungs-, Informations- und Ausbildungskonzepte auch unter Berücksichtigung der Möglichkeiten der Neuen Medien
- Konzepte zur Vermittlung von Kompetenzen zur Bewältigung von Katastrophen und zur Erhöhung der Selbsthilfefähigkeiten in der Bevölkerung

Sicherheitsökonomie

Der Markt für Sicherheitsprodukte und -dienstleistungen mit einem globalen Volumen von ca. 100 Mrd. Euro im Jahr 2008 wächst laut Angaben der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) jährlich um fünf bis sieben Prozent. Auf den europäischen Wirtschaftsraum entfallen ca. 30 Prozent des Gesamtvolumens. Die zivile Sicherheitsforschung wird mit ihren Innovationen dazu beitragen, den Markt für Sicherheitstechnologien und -dienstleistungen weiterzuentwickeln, sodass innovative deutsche Unternehmen sowie forschende Einrichtungen von diesem boomenden Markt profitieren können.

Obwohl mittlerweile ca. 80 Prozent der kritischen Infrastrukturen in privatwirtschaftlicher Hand sind, wird der Markt auch durch die staatliche Nachfrage geprägt. Veränderte Sicherheitsanforderungen erhöhen – trotz knapper werdender Ressourcen öffentlicher Haushalte – den Bedarf, innovative Sicherheitstechnologien und -dienstleistungen einzuführen. Das wird Auswirkungen auf die zukünftige Finanzierung von Sicherheitsleistungen haben und nicht zuletzt auch zu einem verstärkten Ausbau von Sicherheitspartnerschaften führen.

Ziel der Forschung ist es, insbesondere die ökonomischen Folgen und Effekte sicherheitskultureller Wandlungsprozesse und Sicherheitsmaßnahmen zu untersuchen sowie zur Entwicklung neuer Geschäftsmodelle beizutragen.

Forschungsthemen sind unter anderem:

- Ökonomische Betrachtungen von Sicherheitsszenarien bzw. -technologien, insbesondere unter volkswirtschaftlichen Gesichtspunkten
- Untersuchungen zur Bedeutung internationaler Abhängigkeiten beim Zugang zu Schlüsseltechnologien und Rohstoffen für die Gewährleistung ziviler Sicherheit
- Untersuchungen zu den ökonomischen Kosten und zum Nutzen von Sicherheitsmaßnahmen
- Untersuchungen zu den Rahmenbedingungen institutionell übergreifender Kooperations- und Geschäftsmodelle für Sicherheitspartnerschaften
- Analysen zu organisatorischen und rechtlichen Auswirkungen der Verlagerung hoheitlicher Aufgaben bzw. der strukturellen Veränderungen der Sicherheitsarchitektur, einschließlich Untersuchungen zur Übertragbarkeit internationaler Konzepte

Gesellschaftlicher und technischer Wandel

Tief greifende gesellschaftliche Wandlungsprozesse sowie die immer stärkere Vernetzung technischer Systeme und Infrastrukturen stellen eine große Herausforderung für die zivile Sicherheit dar.

Ziel der Forschung ist es, unter Einbeziehung rechtlicher, sozialer und ökonomischer Dimensionen die Entwicklung und Veränderung ziviler Sicherheitslösungen, -kulturen und -architekturen proaktiv mitzugestalten. Forschungsthemen sind unter anderem:

- Untersuchungen zum demografischen und sozialen Wandel und seinen Auswirkungen auf die zivile Sicherheit, zum Beispiel im Hinblick auf die Veränderung gesellschaftlicher Sicherheitsbedürfnisse bzw. der Organisation von Sicherheit sowie der Qualifizierung von Sicherheitsakteuren
- Beiträge zur Ursachenforschung zu politischem Extremismus, Terrorismus und Radikalisierungstendenzen in der Gesellschaft sowie die Entwicklung präventiver Maßnahmen bzw. staatlicher und gesellschaftlicher Gegensteuerungsmöglichkeiten
- Untersuchungen zu den Auswirkungen von Technisierungsprozessen auf Angehörige von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sowie privater Sicherheitsdienstleister. Im Mittelpunkt stehen dabei Veränderungen von Qualifikationsanforderungen sowie organisationsübergreifender Standards
- Untersuchungen und Analysen zu den rechtlichen und gesellschaftlichen Anforderungen und sicherheitsrelevanten Rahmenbedingungen für die Entwicklung datenschutzfreundlicher Technologien unter Berücksichtigung des „privacy by design“-Prinzips

– Untersuchungen und Konzepte zur Gestaltung von Mensch-Technik-Schnittstellen bzw. zu den Auswirkungen von Mensch-Technik-Interaktionen in sicherheitstechnischen Systemen

2.2 Urbane Sicherheit

Menschen wollen sich jederzeit sowohl in ihrem engsten Lebensumfeld als auch auf dem Weg zur Arbeit oder beim Besuch einer Großveranstaltung sicher fühlen. Nicht nur die terroristischen Anschläge in Madrid (2004) und London (2005), sondern auch kriminelle Übergriffe in U- oder S-Bahnen in verschiedenen deutschen Großstädten haben das Thema urbane Sicherheit stärker in das Blickfeld von Politik, Öffentlichkeit und Medien gerückt. Städte und Gemeinden stehen vor der Herausforderung, auch in Zukunft den Schutz der Bürgerinnen und Bürger zu gewährleisten.

Zivile Sicherheitsforschung wird einen Beitrag leisten, Risiken frühzeitig zu erkennen, Unsicherheiten zu verringern und Sicherheit präventiv als integralen Bestandteil einer modernen Stadtgestaltung zu verankern, ohne die Vielfältigkeit und Freiheit städtischen Lebens sowie die informationelle Selbstbestimmung einzuschränken. Dabei sollen nicht nur die Potenziale von Sicherheitstechnologien und -dienstleistungen erforscht, sondern gleichzeitig ihre gesellschaftlichen wie ökonomischen Auswirkungen untersucht werden.

Um diesen Herausforderungen zu begegnen, richten wir die Forschung auf folgende Schwerpunkte aus:

Schutz vor Kriminalität

Kriminalität und Furcht vor Kriminalität können die Lebensqualität in Städten und Gemeinden erheblich einschränken. Auf Basis regionaler Risiko- und Bedarfsanalysen können neue organisatorische und technische Präventionsmöglichkeiten erforscht und kriminalpräventive Maßnahmen fortentwickelt werden. Forschungsthemen sind unter anderem:

– Untersuchungen zu den Ursachen von „Angsträumen“ in Wohn- oder Innenstadtbezirken

– der Einfluss gesellschaftlicher Trends, wie zum Beispiel des demografischen Wandels, auf zukünftige Kriminalitätsentwicklungen in urbanen Lebensräumen

– die Entwicklung von verbesserten Kooperationsformen zwischen den verschiedenen Sicherheitsakteuren, insbesondere in öffentlich-privaten Sicherheitspartnerschaften

„Die resiliente Stadt“

Städte und Metropolen sind aufgrund ihrer hohen Dichte an lebenswichtigen Versorgungsinfrastrukturen und Verkehrsknotenpunkten besonders verwundbar. Auch mit der besten Vorsorge wird es nicht möglich sein, die Bürgerinnen und Bürger in urbanen Ballungsräumen vor allen denkbaren und unvorstellbaren Krisenereignissen zu schützen.

Ziel der Forschung ist die Erhöhung der Resilienz städtischer Lebensräume. Integrierte Stadtplanungs- und Schutzkonzepte machen sie im Katastrophen- oder Krisenfall widerstandsfähiger. Übergreifende Risiko- und Notfallmanagementsysteme helfen, potenzielle Bedrohungen und deren Auswirkungen besser abzuschätzen. Im Krisenfall vernetzen und koordinieren sie effizient alle privaten und staatlichen Sicherheitsakteure. So wird es möglich, die Handlungs- und Funktionsfähigkeit städtischer Infrastrukturen schnellstmöglich wiederherzustellen.

Sicherheit in öffentlichen Einrichtungen

Der freie Zugang zu öffentlichen Institutionen, wie etwa Gemeindeämtern und Bibliotheken ist ein selbstverständlicher Bestandteil des modernen städtischen Lebens. Mutwillige Sachbeschädigungen, Gewalt an Schulen, aber auch die Beeinträchtigung des öffentlichen Lebens durch anonyme Bombendrohungen können schwerwiegende, wenn nicht tragische Folgen nach sich ziehen. Sie beeinflussen das Sicherheitsempfinden der Bürgerinnen und Bürger.

Vor diesem Hintergrund müssen ganzheitliche Präventionsansätze und Schutzmaßnahmen entwickelt werden, die den Ausbau von Sicherheitskompetenzen fördern und eine verbesserte Risiko- und Krisenkommunikation ermöglichen. Ziel ist die Bereitstellung aufbereiteter praxisorientierter Forschungsergebnisse, um die Interventionsmöglichkeiten zum Beispiel in Konflikt- oder Gewaltsituationen an Schulen zu verbessern.

Sicherheit im Wohnumfeld

Kriminalitätsfurcht und Unsicherheitsgefühle können – vor allem bei älteren Menschen – die Lebensqualität im städtischen Raum spürbar einschränken. Nicht selten kommt es durch Vermeidungsverhalten sogar zu einem verstärkten Rückzug in die eigene Wohnung. Gleichzeitig stehen urbane Gemeinschaften in der Zukunft durch die gestiegene Lebenserwartung der Bevölkerung, die Zunahme der Einpersonenhaushalte und nebeneinander existierender ethnischer Milieus vor neuen sozialen Herausforderungen.

Mithilfe der Forschung können neue kooperative, kriminalpräventive Strategien und Schutzkonzepte entwickelt sowie bürgerschaftliche Sicherheitspartnerschaften in urbanen Lebensräumen gefördert werden.

Sicherheit im öffentlichen Personennahverkehr

Der öffentliche Personennahverkehr ist eine der zentralen gesellschaftlichen und wirtschaftlichen Lebensadern urbaner Ballungsräume. Sowohl das dichte Schienen- und Straßennetz, als auch verkehrsnahe Einrichtungen wie Brücken, Tunnel, Haltestellen und Bahnhöfe sind neuralgische Knotenpunkte. Vandalismus, kriminelle Übergriffe auf Fahrgäste und Personal oder Terroranschläge können die Sicherheit und Zuverlässigkeit des öffentlichen Nahverkehrs massiv beeinträchtigen.

Forschungsthemen sind unter anderem:

– integrierte, verkehrsträgerübergreifende Präventionskonzepte und Sicherheitssysteme, die zum Beispiel durch bauliche oder technische Maßnahmen einen besseren Schutz städtischer Verkehrsinfrastrukturen gewährleisten

– optimierte Schulungs- und Qualifizierungskonzepte, die es dem Personal ermöglichen, Krisensituationen frühzeitig zu erkennen und angemessen zu reagieren

– verbesserte Kommunikationskonzepte, die das subjektive Sicherheitsgefühl von Fahrgästen und Personal erhöhen

Sicherheit der Versorgung der Bevölkerung

Die hohe Bevölkerungsdichte in urbanen Räumen und die starke Vernetzung der Versorgungsinfrastrukturen stellen Einsatz- und Rettungskräfte vor besondere technische und organisatorische Herausforderungen. Forschung kann helfen, die Resilienz städtischer Infrastrukturen durch präventive Maßnahmen zu erhöhen. Ein innovatives, akteursübergreifendes Risiko- und Notfallmanagement kann die Versorgung der Bevölkerung mit Trinkwasser, Lebensmitteln und Medikamenten auch im Krisenfall verbessern.

2.3 Sicherheit von Infrastrukturen und Wirtschaft

Deutschland ist als moderne und hochindustrialisierte Gesellschaft von einer Vielzahl funktionierender Infrastrukturen abhängig. Sie versorgen private Haushalte, Unternehmen und öffentliche Verwaltung mit Strom, Wasser sowie Gütern und Dienstleistungen. Diese kritischen Infrastrukturen bilden ein engmaschiges Netz und sind in hohem Maße voneinander abhängig. Bereits geringe Störungen können zu Dominoeffekten führen, die vorübergehende Versorgungsengpässe und hohe volkswirtschaftliche Schäden zur Folge haben können. So kann etwa eine ausreichende Trinkwasserversorgung der Bevölkerung bei einem länger andauernden Stromausfall gefährdet werden.

Staatliche wie privatwirtschaftliche Infrastrukturbetreiber und Unternehmen stehen vor der Herausforderung, das hohe Sicherheitsniveau in Deutschland auch in Zukunft zu erhalten bzw. weiter zu erhöhen. Dazu zählt im Besonderen auch der Schutz technologischer Kernkompetenzen und unternehmerischen Know-hows des Wirtschafts- und Wissensstandorts Deutschland vor organisierter Wirtschaftskriminalität und Industriespionage.

Zivile Sicherheitsforschung wird einen Beitrag leisten, frühzeitig neue Verwundbarkeiten autonomer wie vernetzter Infrastrukturen aufzuzeigen und bestehende Krisenmanagement- und Notversorgungskonzepte weiterzuentwickeln.

Um diesen Herausforderungen zu begegnen, richten wir die Forschung auf folgende Schwerpunkte aus:

Sicherheit kritischer Infrastrukturen

Der Schutz kritischer Infrastrukturen ist eine gesamtgesellschaftliche Herausforderung. Hierzu gehören neben der Energieversorgung die Versorgung mit Trinkwasser und Lebensmitteln, sichere Warenketten sowie die Gesundheitsversorgung, aber auch Verkehrs-, Kommunikations-, Verwaltungsinfrastrukturen sowie kritische Industrieanlagen. Etwa 80 Prozent der kritischen Infrastrukturen werden privatwirtschaftlich betrieben. Deutschland wird den mit der „Nationalen Strategie zum Schutz kritischer Infrastrukturen“ erfolgreich eingeschlagenen Weg der vertrauensvollen und konstruktiven Kooperation fortsetzen und die Zusammenarbeit der relevanten Akteure aus Staat und Wirtschaft vertiefen und ausbauen.

Natürliche, technische oder gesellschaftliche Risiken, aber auch die weiter wachsende Vernetzung sowohl innerhalb als auch zwischen einzelnen Infrastrukturen haben zu einer erhöhten Verletzlichkeit geführt. Forschungsthemen sind unter anderem:

– risikobasierte Resilienzstrategien, die im Sinne eines All-Gefahren-Ansatzes sowohl die Verbesserung der Widerstands- und Regenerationsfähigkeit einzelner kritischer Infrastrukturen als auch des Gesamtsystems vernetzter Infrastrukturen anstreben

– infrastrukturübergreifende Simulationen und Vorhersagemodelle, die dabei helfen, die Robustheit kritischer Infrastrukturen langfristig sicherzustellen und das Management von Interdependenzen zu erleichtern

– technische Lösungen sowie Krisenmanagement- und Notversorgungskonzepte, die eine schnellstmögliche Wiederherstellung geschädigter Infrastrukturen ermöglichen bzw. eine vorübergehende Notversorgung mit lebenswichtigen Gütern und Dienstleistungen gewährleisten

– technische Lösungen und Maßnahmen, die – integriert, mobil oder auch autonom einsetzbar – den Schutz kritischer Infrastrukturen vor den Folgen von Naturkatastrophen, terroristischen Angriffen oder neuen technischen Risiken verbessern, einschließlich Untersuchungen zu den Auswirkungen elektromagnetischer Impulse bzw. geomagnetischer Stürme

Sicherheit der Infrastrukturen von morgen

Durch neue technologische Entwicklungen werden Infrastrukturen künftig nicht nur stärker vernetzt, sondern auch dezentraler organisiert sein. Beispiele sind das „Internet der Dinge“, der Einzug der Smart-Grid-Technologie in die Energieversorgung, der kontinuierliche Ausbau des e-Governments oder auch der vermehrte Einsatz telemedizinischer Anwendungen im Gesundheitswesen. Neben einem damit verbundenen Gewinn an Komfort, Sicherheit und Mobilität können aber auch neue Verwundbarkeiten entstehen.

Deshalb ist es erforderlich, frühzeitig integrierte Design- und Resilienzstrategien („security by design“) zu entwickeln, die der informationellen Selbstbestimmung Rechnung tragen („privacy by design“). Risikoanalysen und

Simulationen helfen, potenzielle Sicherheitslücken zu erkennen und geeignete Lösungen zu entwickeln.

Betriebliches Kontinuitätsmanagement in Katastrophenlagen

In Zeiten weltumspannender Liefer- und Wertschöpfungsketten ist die Wettbewerbsfähigkeit Deutschlands als führende Industrienation in der Mitte Europas eng mit der kontinuierlichen Verfügbarkeit kritischer Infrastrukturen und internationaler Waren-, Verkehrs- und Rohstoffflüsse verbunden. Für Unternehmen ebenso wie für kritische Infrastrukturbetreiber stellen Natur- und Umweltkatastrophen, Pandemieausbrüche oder Großunfälle erhebliche Risiken dar. Diese können zu schwerwiegenden Unterbrechungen von Produktions- und Dienstleistungsprozessen führen und hohe volkswirtschaftliche Schäden zur Folge haben.

Ein ganzheitliches Kontinuitätsmanagement basiert auf institutionenübergreifender Kommunikation und Kooperation. Neue Trainings- und Sensibilisierungsansätze befähigen Unternehmen und ihre Mitarbeiterinnen und Mitarbeiter, Katastrophenlagen besser zu bewältigen. Ziel ist es, Produktionsstandorte und Mitarbeiterinnen und Mitarbeiter zu schützen und kritische Unternehmensinfrastrukturen und -prozesse zeitnah und kosteneffizient wiederherzustellen.

Sicherheit des zivilen Luftverkehrs/ Luftfrachtsicherheit

Der zivile Luftverkehr ist ein wesentlicher Faktor der wirtschaftlichen Stärke und gesellschaftlichen Mobilität Deutschlands. Allein von deutschen Flughäfen aus wurden im Jahr 2010 über 190 Millionen Passgiere und etwa 4,4 Mio. t Güter in die ganze Welt transportiert. Mit dem weiterhin steigenden Passagier- und Frachtaufkommen und dem Ausbau des Luftverkehrsnetzes wachsen auch die Herausforderungen im Bereich Luftverkehrs- bzw. Luftfrachtsicherheit. Vereitelte Anschlagsversuche auf Passagier- und Frachtmaschinen, aber auch durch Naturkatastrophen ausgelöste Störungen des Flugbetriebs haben schmerzhaft die Verletzlichkeit des internationalen Luftverkehrs vor Augen geführt. Das stellt Flughafenbetreiber, Fluggesellschaften ebenso wie Behörden und private Sicherheitsdienstleister vor immer höhere technische und organisatorische Herausforderungen bei der Kontrolle von Passagieren, Personal, Gepäckstücken oder Luftfrachtcontainern. Zudem muss auch die Sicherheit von Flugkontroll- und Sicherheitseinrichtungen sowie angrenzender Bereiche um Flughäfen gewährleistet werden.

Um auch in Zukunft die sichere und reibungslose Abwicklung des zivilen Luftverkehrs zu gewährleisten und dabei proaktiv auf neue Bedrohungslagen reagieren zu können, müssen verstärkt innovative Sicherheitskonzepte entwickelt werden. Forschungsthemen sind unter anderem:

– vollautomatisierte und berührungsfreie Methoden des Personen- und Frachtscreenings
– luft- und bodengestützte Überwachung und Sicherung von Flughäfen, Flugsicherungseinrichtungen, geparktem Fluggerät und Kommunikationseinrichtungen
– akteursübergreifende Krisenmanagementsysteme
– verbesserte Schulungs- und Sensibilisierungsmaßnahmen

Maritime Sicherheit

Sichere Seewege sind nicht nur für den Fährverkehr, sondern auch für den internationalen Warenaustausch von elementarer Bedeutung. Der überwiegende Teil des globalen Gütertransfers wird über den Seeweg abgewickelt. Laut Statistischem Bundesamt wurden im Jahre 2010 in den deutschen Seehäfen ca. 276 Mio. t Güter umgeschlagen. Häfen sind ebenso wie Personen- bzw. Frachtschiffe verstärkt Gefahren ausgesetzt. Dazu zählt insbesondere die wachsende Problematik moderner Piraterie bzw. des maritimen Terrorismus, aber auch Risiken, die von potenziellen Folgen regionaler Umwelt- oder Naturkatastrophen ausgehen können. Unterbrechungen von Hauptrouten des internationalen Seefrachtverkehrs oder die zeitweilige Schließung von Häfen können die Folge sein. Zudem sind in den letzten Jahren die Gefahren des Missbrauchs von Containern für den Schmuggel von illegalen Waffen, Sprengstoffen, Drogen und anderen Gefahrstoffen gestiegen.

Vor diesem Hintergrund müssen Sicherheitslösungen entwickelt werden, die eine lückenlose Kontrolle der Integrität von Waren und Containern entlang der gesamten Transportkette ermöglichen. Ganzheitliche Konzepte werden den Schutz maritimer Infrastrukturen und Logistikprozesse nachhaltig verbessern.

Schutz vor Wirtschaftskriminalität, Produktpiraterie und Industriespionage

Deutsche Unternehmen sind mit ihrer Innovationskraft und ihrer starken Präsenz auf internationalen Märkten nicht nur von einer gesicherten Rohstoff- und Energieversorgung abhängig, sondern immer mehr auf den Schutz ihres Know-hows sowie die Sicherheit ihrer Produktionsstandorte und Mitarbeiterinnen und Mitarbeiter im In- und Ausland angewiesen. Besonders der Produktionsfaktor Wissen gewinnt durch die weltweite Vernetzung an Bedeutung. Große Konzerne ebenso wie mittelständische Betriebe müssen sich zunehmend vor innerbetrieblichen und externen Gefährdungen schützen, die Folgen organisierter Wirtschaftskriminalität, Produktpiraterie und Wirtschafts- und Industriespionage sind.

Deshalb müssen zur Stärkung der Sicherheitskompetenzen in den Unternehmen präventive Schutzlösungen entwickelt werden. Forschungsthemen sind unter anderem:

– ein innovatives, standortübergreifendes Krisenmanagement, um konkrete Bedrohungen für unternehmenskritische Prozesse frühzeitiger zu erkennen und einen bestmöglichen Schutz von Produkten, Know-how und Mitarbeiterinnen und Mitarbeiter zu gewährleisten

– innovative Lösungen zur schnellen Identifizierung von Produktfälschungen und zur Nachverfolgung der Produktions- und Distributionsprozesse und -wege

Neue Sicherheitsdienstleistungen

Sicherheitsdienstleistungen sind ein wichtiges Element der modernen staatlichen und unternehmerischen Sicherheitsvorsorge. Gestiegene Sicherheitsanforderungen und die fortschreitende Privatisierung kritischer Infrastrukturen haben vor dem Hintergrund knapper werdender Ressourcen zu einer stärkeren Aufgabenteilung zwischen öffentlicher Hand und privater Wirtschaft geführt. Im Rahmen von Ordnungs- und Sicherheitspartnerschaften decken private Sicherheitsdienstleister zusammen mit Infrastrukturbetreibern, Polizei und kommunalen Behörden bereits heute ein immer breiteres Spektrum an Sicherheits- und Schutzaufgaben ab. Das erhöht den Bedarf an qualifiziertem Personal, modernen Sicherheitstechnologien und flexiblen Kooperations- und Geschäftsmodellen.

Forschung wird die Entwicklung nutzerorientierter Dienstleistungsmodelle und -standards vorantreiben. Die Einführung neuer Technologieplattformen wird neue Sicherheitsdienstleistungen ermöglichen. Neue Qualifizierungs- und Sensibilisierungskonzepte werden die Qualität, Effizienz und Akzeptanz von Sicherheitsdienstleistungen steigern.

2.4 Schutz und Rettung von Menschen

Die Bürgerinnen und Bürger vor Gefahren zu schützen und für ihre Sicherheit Sorge zu tragen, ist eine der Kernaufgaben staatlichen Handelns. Dies gilt insbesondere mit Blick auf Risiken und Großschadenslagen, die durch Naturkatastrophen – wie Hochwasserlagen oder Stürme – oder durch technisches und menschliches Versagen verursacht werden. Aktuelle Forschungsergebnisse zeigen, dass auch in Deutschland die Folgen des Klimawandels zu einer Zunahme witterungsbedingter Naturkatastrophen führen können.

Zivile Sicherheitsforschung wird einen Beitrag leisten, unter Einbindung aller staatlichen und gesellschaftlichen Akteure den Schutz der Bevölkerung und ihrer Lebensgrundlagen auf hohem Niveau sicherzustellen. Um diesen Herausforderungen zu begegnen, werden wir die Forschung am Resilienzzyklus ausrichten und folgende Schwerpunkte setzen:

Krisen- und Einsatzmanagement

Deutschland verfügt über einen gut funktionierenden Bevölkerungsschutz mit einem weltweit einzigartigen Hilfeleistungspotenzial. Maßgeblichen Anteil daran haben die über 1,8 Millionen hoch qualifizierten Schutz- und Rettungskräfte auf Bundes-, Länder- und kommunaler Ebene und der hohe technische Ausrüstungsstandard in Feuerwehr, Polizei, Rettungsdiensten und Katastrophenschutzeinheiten. Gleichwohl stehen die haupt- und ehrenamtlichen Einsatzkräfte und Helfer immer häufiger vor der Aufgabe, zunehmend komplexere Großschadenslagen, auch im Rahmen internationaler humanitärer Hilfsaktionen, bewältigen zu müssen. So können sich durch Extremwetterereignisse, Umweltkatastrophen oder technische Großunfälle ausgelöste – zunächst örtlich begrenzte – Schadenslagen schnell zu überregionalen oder sogar grenzüberschreitenden Katastrophen ausweiten.

Um den Schutz der Bevölkerung und die Einsatzfähigkeit aller Schutz- und Rettungskräfte auch zukünftig auf hohem Niveau sicherzustellen, muss, aufbauend auf umfassenden Risikoanalysen, ein geeignetes Krisenmanagement entwickelt werden. Präventive Resilienz-, Frühwarn- und Schulungskonzepte müssen mit dem konsequenten Ausbau technischer und organisatorischer Reaktionskapazitäten verbunden werden. Forschungsthemen sind unter anderem:

– intelligente Systeme zur Entscheidungsunterstützung, die auch mithilfe von Simulation und Modellierung bereits im Vorfeld oder im Verlauf von Großschadenslagen Gefahren und Risiken abschätzen helfen

– Koordinationssysteme, die zum Beispiel durch vernetzte Lagedarstellungen und Ad-hoc-Kommunikationssysteme die institutions- oder auch grenzübergreifende Koordination von Rettungseinsätzen oder notwendige Evakuierungsmaßnahmen erleichtern

– integrierte Planungsinstrumente sowie verbesserte Informations- und Ausbildungskonzepte, die unter Einbindung aller Sicherheitsakteure die Vorbereitung und Durchführung von Großveranstaltungen unterstützen und in Krisenfällen ein umfassendes Einsatz- und Konfliktmanagement ermöglichen

Moderne Einsatz-, Kommunikations- und Rettungssysteme müssen hinsichtlich Robustheit, Leistungsfähigkeit, Interoperabilität und Handhabbarkeit an den Ergebnissen der Risikobewertungen ausgerichtet und optimiert werden. Forschungsthemen sind unter anderem:

– die Optimierung der Reaktionskapazitäten zur schnellen und koordinierten Bewältigung eines Massenanfalls von Verletzten, insbesondere bei Großschadenslagen

– die Entwicklung autonomer Rettungs- und Hilfssysteme und intelligenter Mensch-Maschine-Schnittstellen, die zum Beispiel die Suche und Rettung von Verschütteten erleichtern

– technische und organisatorische Hilfsmittel für Rettungs- und Einsatzkräfte, um zum Beispiel die Folgen von Extremwetterereignissen besser bewältigen zu können oder die ambulante Versorgung pflegebedürftiger Menschen im Katastrophenfall sicherzustellen

– moderne Ausbildungs- und Trainingsmethoden bzw. -technologien für vernetzte und organisationsübergreifende Schulungen und Übungen zum Krisenmanagement

Anpassungsstrategien an gesellschaftlichen Wandel

Der Katastrophenschutz muss auf die langfristige Veränderung von Einsatzbildern und Rahmenbedingungen vorbereitet werden, die sich durch tief greifende gesellschaft-

liche Wandlungsprozesse ergeben. So wird beispielsweise die im Mai 2011 gesetzlich in Kraft getretene Aussetzung des Zivil- bzw. Ersatzdienstes unmittelbare Auswirkungen auf die Rekrutierungsmöglichkeiten ehrenamtlicher Helfer haben. Auch der demografische Wandel stellt eine große Herausforderung dar. So wird die Bevölkerungsgruppe im Erwerbsalter zwischen 20 und 65 Jahren bis 2060 um ca. ein Drittel gegenüber dem heutigen Stand abnehmen.

Um dem erwarteten Fachkräfte- und Helfermangel begegnen zu können, müssen neue Qualifizierungs- und Ausbildungskonzepte sowie Beteiligungsmodelle entwickelt werden. Sie sind Voraussetzung für die langfristige Sicherung des freiwilligen bürgerschaftlichen Engagements.

Bürgerinnen und Bürger als Betroffene und Helfer

Staatliche und private Sicherheitsakteure und Hilfsorganisationen können die zukünftigen Herausforderungen des nationalen wie internationalen Katastrophenschutzes nur meistern, wenn sie ihre Ziele, Prozesse und Strukturen ebenso wie ihre Fähigkeiten und Einsatzmittel stärker miteinander vernetzen. Das kann jedoch nur gelingen, wenn die Bürgerinnen und Bürger nicht nur als Betroffene wahrgenommen und informiert, sondern auch unmittelbar als Helfer einbezogen werden. Deshalb müssen Kommunikationsstrategien und Selbstschutzkonzepte entwickelt bzw. ausgebaut werden, die sowohl die Krisenkommunikation bei Großschadenslagen verbessern, aber auch die Selbsthilfefähigkeiten in der Bevölkerung erhöhen. Beispielsweise können die Neuen Medien helfen, Bürgerinnen und Bürgern die notwendigen Vorsorge- und Bewältigungskompetenzen zu vermitteln. Sie können aber auch genutzt werden, um die Aufklärung und Frühwarnung bei Krisenereignissen interaktiver zu gestalten.

2.5 Schutz vor Gefahrstoffen, Epidemien und Pandemien

Der Schutz von Menschen und Infrastrukturen vor chemischen, biologischen, radiologischen, nuklearen Gefahren und Explosivstoffen (CBRNE-Gefahren) sowie Epidemien und Pandemien ist zentrale Komponente eines modernen Bevölkerungsschutzes. CBRNE-Gefahrstoffe, zu denen Industriechemikalien ebenso zählen wie Infektionserreger, Toxine oder radioaktive Stoffe, können ohne Vorwarnung freigesetzt werden und schnell zu Schadenslagen mit katastrophalen Ausmaßen führen. Die auch in Deutschland spürbaren Auswirkungen der Schweine- oder Vogelgrippe haben vor Augen geführt, dass Infektionserreger in Zeiten hoher Mobilität innerhalb kürzester Zeit weltweite Pandemielagen auslösen können. Sowohl bei CBRNE-Ereignissen als auch bei größeren Epidemien und im Falle einer von der Weltgesundheitsorganisation WHO ausgerufenen Pandemie handelt es sich um dynamische und zeitkritische Gefahrensituationen mit hohem Eskalationspotenzial.

Zivile Sicherheitsforschung wird dazu beitragen, CBRNE-Risiken und pandemische Bedrohungen frühzeitig zu erkennen und die schnelle und zielgerichtete Reaktion der zuständigen Behörden und Einsatzkräfte weiter zu optimieren. Daher richten wir die Forschung auf folgende Schwerpunkte aus:

Schutz vor CBRNE-Gefahrenlagen

CBRNE-Gefahrenlagen stellen die zuständigen Behörden und die vor Ort eingesetzten Helfer der Feuerwehren, Rettungsdienste und Katastrophenschutzeinheiten vor große fachliche und technische Herausforderungen. Der technologische Fortschritt aber auch die globale Vernetzung haben nicht nur die Möglichkeiten zur Herstellung, Verbreitung und zum Missbrauch von CRBNE-Gefahrstoffen erheblich erweitert, sondern auch die Verwundbarkeit vernetzter Systeme erhöht. Damit wachsen die Risiken, die von illegalem Schmuggel, terroristisch motiviertem Einsatz von CBRNE-Gefahrstoffen, oder auch der industriellen Herstellung, Lagerung, dem Transport und der Anwendung dieser Stoffe ausgehen.

Um zukünftig neuen Gefährdungspotenzialen und den häufig flächendeckenden Auswirkungen der CBRNE-Krisenszenarien angemessen begegnen zu können, müssen bestehende Risikobewertungs-, Schutz- und Notfallkonzepte fortentwickelt werden. Forschungsthemen sind unter anderem:

- leistungsfähigere Detektionssysteme sowie verbesserte Probenahme- und Aufbereitungsverfahren, die – mobil einsetzbar oder aus sicherer Entfernung – ein breites Spektrum von CBRNE-Gefahrstoffen detektieren können sowie Technologien zur Dosiserfassung
- verbesserte Konzepte für die medizinische Versorgung bei einem Massenanfall Verletzter oder Erkrankter bei CBRNE-Lagen. Dazu zählen u. a. Themen wie Triagierung, Diagnostik, Dekontamination und Behandlung (präklinisch und klinisch)
- Sensibilisierungs- und Selbstschutzstrategien, die gezielt die Selbsthilfefähigkeiten der Bevölkerung stärken und verbesserte Aus- und Fortbildungskonzepte für Einsatzkräfte und Führungskräfte, die auf neueste technische und organisatorische Entwicklungen abgestimmt sind

Schutz vor Pandemien und neuen Infektionskrankheiten

Trotz aller Fortschritte in der medizinischen Versorgung und des Wissens über die Mikrobiologie von Krankheitserregern und Überträgern können Pandemien und Seuchen auch heute die Gesundheit und die Nahrungsmittelgrundlage aller Bürgerinnen und Bürger bedrohen. Der weltweite Warenaustausch und Reiseverkehr, aber auch veränderte klimatische Bedingungen begünstigen die Verbreitung und Übertragung von Infektionskrankheiten bzw. neuartigen Erregern. Die SARS-Epidemie 2003 und die Pandemiewellen der Schweine- und Vogelgrippe haben gezeigt, dass bei großflächigen Seuchenausbrüchen mit extremen Belastungen insbesondere der Infrastrukturen und Einrichtungen des öffentlichen Gesundheitswe-

sens zu rechnen ist. Gerade in modernen Industriegesellschaften besteht das Risiko, dass im Falle hoher Erkrankungsraten lebenswichtige Infrastrukturleistungen nicht mehr aufrechterhalten werden können und die Funktionsfähigkeit der Volkswirtschaft gefährdet ist.

Es gilt, die wissenschaftlichen Grundlagen für den gesundheitlichen Bevölkerungsschutz einschließlich überregionaler Pandemieplanungen weiterzuentwickeln und dabei bestehende Expertennetzwerke wie die Nationale Forschungsplattform für Zoonosen einzubinden. Notwendig sind verbesserte Risiko- und Notfallstrategien und evidenzbasierte Bewertungsverfahren, um das Krisenmanagement bei der Bekämpfung und Eindämmung von Seuchen weiter zu verbessern. Angepasste präventive Maßnahmen und integrierte Monitoring- und Abwehrkonzepte werden es auf der Grundlage neuester Ergebnisse aus der Gesundheitsforschung ermöglichen, neuartige Krankheitserreger und potenzielle Überträger frühzeitig zu identifizieren.

2.6 Informationen zu Aktivitäten des BMBF im Bereich IT-Sicherheitsforschung

Informations- und Kommunikationstechnologien (IKT) sind die digitalen Nervenstränge unserer Gesellschaft. Von ihrem zuverlässigen Funktionieren und von dem Vertrauen in die Sicherheit der IKT-Systeme hängen inzwischen weite Bereiche des gesellschaftlichen und wirtschaftlichen Lebens ab. Allerdings nehmen die Anzahl, die Intensität und das Niveau von Angriffen im Cyberraum auf Nutzer wie auch auf lebensnotwendige Infrastrukturen seit Jahren mit unverminderter Geschwindigkeit zu. Sie beeinträchtigen nicht nur die informationelle Selbstbestimmung des Einzelnen, sondern führen auch zu großen wirtschaftlichen Verlusten.

Um diesen Herausforderungen zu begegnen, hat das Bundesministerium für Bildung und Forschung im Forschungsprogramm IKT 2020 (Rahmenprogramm „Schlüsseltechnologien und Querschnittsmaßnahmen“) einen Schwerpunkt im Bereich IT-Sicherheitsforschung gesetzt. Zwei dieser Aktivitäten werden im Folgenden nachrichtlich vorgestellt.

(a) Das Bundesministerium für Bildung und Forschung und das Bundesministerium des Innern haben im Jahr 2008 ein gemeinsames Arbeitsprogramm IT-Sicherheitsforschung mit einer Laufzeit bis zunächst 2013 aufgelegt, das die Forschung auf folgende Schwerpunkte ausrichtet:

Sicherheit in unsicheren Umgebungen

Die Entwicklung der IKT-Welt ist geprägt von zunehmender Vernetzung, hoher Mobilität, einer exponentiell ansteigenden Zahl von angeschlossenen Geräten und einer zunehmenden Verschmelzung von realer Welt und Cyberwelt. Analysen zur Gesamtsystemsicherheit scheitern an der enormen Komplexität. Stattdessen müssen IKT-Systeme derart entworfen oder nachträglich gehärtet werden, dass ihr Betrieb auch in unsicheren Umgebungen in einem vertrauenswürdigen Zustand möglich ist.

Forschungsthemen sind unter anderem:

- Schutz mobiler Kommunikationsbeziehungen vor Angriffen über die Netzinfrastruktur
- Verfahren zur Detektion und Abwehr von Schadsoftware in mobilen Endgeräten
- Weiterentwicklung von Analyseverfahren wie virtualisierten Umgebungen und sogenannten Honeynets auf die Bedürfnisse mobiler Umgebungen
- Möglichkeiten zur betreiberunabhängigen und netzübergreifenden, sicheren Kommunikation in Mobilfunknetzen

Schutz von Internet-Infrastrukturen

Die überwältigende Erfolgsgeschichte des Internets war nicht vorherzusehen. Entsprechend wurden bei seiner Entwicklung Sicherheitsaspekte nur nachrangig betrachtet, während das Hauptaugenmerk der Netzverfügbarkeit unter der Annahme friedlich kooperierender Netzteilnehmer galt. Da das Internet und vergleichbar große Netze prinzipiell nicht umfassend gegen Angriffe geschützt werden können, gilt es, die Erkennung von Anomalien und die möglichst frühzeitige Eindämmung von Netzangriffen zu ermöglichen.

Forschungsthemen sind unter anderem:

- Technologien und Verfahren zur Angriffsprävention und zur Frühwarnung, die es ermöglichen, auf gerade erst entstehende Gefährdungen aktiv zu reagieren und ihre Auswirkungen einzudämmen
- Maßnahmen zur Verteilung von Detektions-, Abwehr- und Selbstheilungsmechanismen, um heute vorherrschende singuläre Schwachstellen zu reduzieren und eine Nutzung der IT-Infrastrukturen auch während und nach groß angelegten Angriffsszenarien zu ermöglichen

Eingebaute Sicherheit

Instrumente der IT-Sicherheit werden heute noch überwiegend reaktiv eingesetzt. Erst nach Bekanntwerden von Schwachstellen werden Updates verteilt, Firewalls reglementieren den Datenverkehr und Virenscanner versuchen, mit immer neuen Methoden Schadcodes zu erkennen. Auf lange Sicht hin ist IT-Sicherheit jedoch nur zu gewährleisten, wenn die Sicherheitsanforderungen bereits bei der Systementwicklung eine zentrale Rolle spielen. Zusätzlich müssen Systeme in die Lage versetzt werden, unerlaubte Modifikationen, wie sie bei einer Infektion auftreten, selbst zu erkennen und auf diese reagieren zu können.

Forschungsthemen sind unter anderem:

- Innovative Methoden des Trusted Computing, die dazu beitragen, während der Laufzeit den vertrauenswürdigen und sicheren Systemzustand auf verschiedensten Hardwareplattformen – vom Bürorechner bis zum RFID-Transponder – zu erkennen und zu gewährleisten

– Sicherheitsaspekte bei sogenannten feldprogrammierbaren Gate-Arrays (FPGA): Sie bieten eine hohe Leistungsfähigkeit bei gleichzeitig hoher Flexibilität. Damit einher geht besonders im Hochsicherheitsbereich die Notwendigkeit, Sicherheitsfunktionen sicher, dauerhaft und nachweisbar separiert zu speichern, und Funktionen, die auf physikalischen Effekten beruhen, sicher zu implementieren

Neue Herausforderungen zum Schutz von IT-Systemen und zur Identifikation von Schwachstellen

Durch den technischen Fortschritt zum Beispiel bei der Quanteninformatik können zukünftig neuartige Angriffsszenarien auf Verfahren entstehen, die heute noch als vertrauenswürdig und sicher gelten. Durch die Entwicklung neuer Methoden, die auch potenzielle technologische Entwicklungen antizipieren, soll ein langfristiges Sicherheitsniveau geschaffen werden.

Ebenfalls im Fokus der Forschung stehen indirekt ausgeführte Angriffe, sogenannte Seitenkanalattakken. Durch diese werden als sicher angesehene Verschlüsselungstechnologien attackiert, beispielsweise durch Messungen ihres Stromverbrauchs oder der elektromagnetischen Abstrahlung. Durch ein angepasstes Systemdesign sollen Bausteine geschaffen werden, die von sich aus gegen derartige Angriffe immun sind.

Forschungsthemen sind unter anderem:

– Seitenkanalangriffe, deren Funktionsfähigkeit bisher hauptsächlich gegen isolierte Sicherheitskomponenten untersucht wurde, sollen auch auf ihre Einsetzbarkeit gegenüber sogenannten FPGA-Lösungen und eingebetteten Systemen untersucht werden und ggf. Abwehrmechanismen gegen sie entwickelt werden

– Forensische und analytische Werkzeuge, besonders zur Analyse im laufenden Betrieb und mit der Fähigkeit zur dynamischen Codeanalyse, sollen entwickelt und verbessert werden

– Neuartige Kryptoverfahren, die gegen mögliche Entwicklungen in der Quanteninformatik resistent sind, sollen erforscht und prototypisch umgesetzt werden

(b) Ein weiterer Schwerpunkt zur IT-Sicherheit im Forschungsprogramm IKT 2020 (Rahmenprogramm „Schlüsseltechnologien und Querschnittsmaßnahmen“) ist die Förderung von Kompetenzzentren zur Cybersicherheit. Im Frühjahr 2011 wurden drei Zentren ausgewählt, damit sich Deutschland den großen Zukunftsfragen der Cybersicherheit langfristig stellen kann. Die Zentren bündeln thematisch und organisatorisch die besten Hochschulen und außeruniversitären Forschungseinrichtungen auf dem Gebiet der Cybersicherheitsforschung in Deutschland. Inhaltliche Schwerpunkte sind neben Themen wie der Sicherheit von Software, IT-Systemen, Smart Grids und Cloud Computing insbesondere auch gesellschaftlich relevante Aspekte des Internets, wie etwa der Schutz der persönlichen Daten und Privatsphäre des Bürgers oder der Aufbau einer Vertrauenskultur im Internet.

Weitere Informationen zur IT-Sicherheitsforschung des BMBF erhalten Sie unter www.it-sicherheitsforschung.de.

3 Förderinstrumente und Maßnahmen

3.1 Gemeinsam innovative Lösungen für konkrete Herausforderungen entwickeln

Szenarienorientierte Sicherheitsforschung

Ein wesentlicher Schwerpunkt des Rahmenprogramms liegt in der Förderung szenarienorientierter Fragestellungen. Damit stellen wir sicher, dass die Forschung am Problemlösungsbedarf von Endnutzern und Anwendern ausgerichtet wird. Ausgehend von globalen und gesellschaftlichen Herausforderungen der zivilen Sicherheit stützen sich die Szenarien auf konkrete Risiko- und Bedrohungsanalysen und berücksichtigen sicherheitsökonomische Aspekte ebenso wie die gesellschaftliche Dimension der zivilen Sicherheit.

Szenarien bieten eine akteur- und disziplinübergreifende Plattform, auf der Wissenschaft, Industrie sowie privatwirtschaftliche Endnutzer und Behörden entlang der gesamten Innovationskette zusammenarbeiten. Für die Erarbeitung ganzheitlicher und umsetzungsfähiger Sicherheitslösungen ist es notwendig, alle relevanten Disziplinen aus den Technik-, Natur- und Gesellschaftswissenschaften einzubinden und auf gemeinsame Anwendungsziele auszurichten. Deswegen ist es unser ausdrückliches Ziel, die Inter- und Transdisziplinarität in den Projekten vor allem durch die gleichberechtigte Integration gesellschaftswissenschaftlicher Forschung zu fördern. Denn es geht nicht um die Entwicklung des technologisch Machbaren, sondern um die Einführung ethisch, rechtlich und ökonomisch verantwortbarer Innovationen.

Die Szenarienorientierung vermeidet isolierte Einzellösungen. Sie ermöglicht anwendungsnahe Systeminnovationen, aus denen sich praxistaugliche Sicherheitsprodukte und -dienstleistungen erfolgreich entwickeln lassen, die sich am Bedarf der Endnutzer orientieren und zu einer freiheitlichen Gesellschaft passen.

Querschnittsorientierte Sicherheitsforschung

Neben der szenarienorientierten Forschung setzen wir einen weiteren Schwerpunkt in der Förderung querschnittsorientierter Fragestellungen.

Im Mittelpunkt stehen zum einen übergreifende Forschungsansätze, die naturwissenschaftlich-technisches Basiswissen erschließen und aus bestehenden und neuen Basistechnologien innovative Sicherheitslösungen entwickeln. Die Anwendungsnähe und Praxistauglichkeit wird durch Einbeziehung der gesamten Innovationskette und die angemessene Berücksichtigung gesellschaftlicher Fragestellungen gewährleistet.

Zum anderen werden übergreifende Forschungsansätze zur gesellschaftlichen Dimension der zivilen Sicherheits-

forschung aufgegriffen. So können Fragen zur Akzeptanz spezifischer Technologieentwicklungen und zum Datenschutz ebenso untersucht werden wie grundlegende Fragestellungen zur Sicherheitskultur und -architektur. Die Anschlussfähigkeit wird auch hier regelmäßig durch die Einbindung der Endnutzer gewährleistet.

Programmumsetzung

Das Rahmenprogramm „Forschung für die zivile Sicherheit“ baut auf der im Jahr 2007 gestarteten ersten Programmphase auf und ist für eine Laufzeit bis 2017 ausgelegt. Als lernendes Programm bildet es den Rahmen für eine längerfristig ausgerichtete flexible Förderpolitik, die auf Basis der Erfahrungen bei der Programmdurchführung und sich ändernder Herausforderungen weiterentwickelt wird.

Das Rahmenprogramm wird im Wesentlichen durch öffentliche Bekanntmachungen umgesetzt, in denen für bestimmte Themenfelder zur Einreichung von Projektvorschlägen aufgerufen wird. In der Bekanntmachung werden der jeweilige Themenschwerpunkt präzisiert und die Fördermodalitäten verbindlich festgelegt. Gefördert werden vorrangig Verbundprojekte, die endnutzer- oder industriegeführt sein sollen und alle notwendigen Forschungsdisziplinen einbeziehen. Je nach Zielsetzung der jeweiligen Fördermaßnahme können auch Einzelvorhaben und Studien gefördert werden. In einem wettbewerbsorientierten Verfahren werden die besten Projektvorschläge ausgewählt. Die Laufzeit der geförderten Verbundvorhaben wird in der Regel drei Jahre betragen.

Aufbauend auf den Erfolgen der ersten Programmphase wollen wir die Beteiligung von kleinen und mittleren Unternehmen (KMU) in der Sicherheitsforschung weiter ausbauen. Gerade die gemeinsame Forschung in Verbundprojekten ermöglicht KMU den unmittelbaren Kontakt zu exzellenten Forschungseinrichtungen. Darüber hinaus erhalten sie durch die Kooperation mit international agierenden Konzernen Zugang zu Schlüsselanwendern und Märkten.

Es ist vorgesehen, die Umsetzung der zivilen Sicherheitsforschung mittels einer ex-post Evaluation zu analysieren. Darüber hinaus wird das Programm durch einen wissenschaftlichen Programmausschuss begleitend evaluiert. Ihm gehören Expertinnen und Experten aller relevanten Wissenschaftsdisziplinen, der Industrie sowie privatwirtschaftlicher Infrastrukturbetreiber und öffentlicher Behörden und Organisationen mit Sicherheitsaufgaben an. Als unabhängiges Gremium berät der Programmausschuss das BMBF bei der strategischen und inhaltlichen Ausrichtung der zivilen Sicherheitsforschung. Der Ausschuss soll den Wissenstransfer in die Praxis sowie die Verzahnung der deutschen mit den europäischen Aktivitäten im Bereich der zivilen Sicherheitsforschung unterstützen.

Die Kooperation der Bundesressorts ist integraler Bestandteil des Rahmenprogramms. Zentrale Akteure der zivilen Sicherheitsforschung sind insbesondere das Bundesministerium des Innern, das Wirtschafts-, das Verkehrs- und das Gesundheitsressort. Die ressortübergreifende Abstimmung erfolgt über den Ressortkreis Sicherheitsforschung, in welchem alle zuständigen und am Rahmenprogramm beteiligten Bundesministerien Vertreter entsenden können.

3.2 Innovationstransfer unterstützen

Der Markt ziviler Sicherheitsprodukte und -dienstleistungen ist von besonderen Rahmenbedingungen geprägt. Innovative Sicherheitslösungen müssen sowohl den Anforderungen und Bedürfnissen staatlicher oder privater Endnutzer entsprechen als auch die Balance zwischen Sicherheit und Freiheit wahren. Denn nur Innovationen, die sich in der Gesellschaft und am Markt bewähren, führen letztendlich auch zu mehr Sicherheit.

Forschung ist immer mit einem hohen Erfolgsrisiko verbunden. Nicht alle ursprünglich vielversprechenden Forschungsansätze erweisen sich im Projektverlauf als realisierbar. Erfolgreiche Forschungsprojekte werden wir mit geeigneten Maßnahmen beim Transfer ihrer Ergebnisse in marktfähige Produkte und Dienstleistungen unterstützen.

Dialog zwischen den Akteuren

Grundvoraussetzung für den erfolgreichen Innovationstransfer ist der kontinuierliche Dialog zwischen den Akteuren der zivilen Sicherheitsforschung. In den Verbundprojekten ist der Dialog zwischen den Akteuren ein projektimmanenter Bestandteil. Forschung, Wirtschaft und Endnutzer entwickeln in den Projekten nicht nur gemeinsam umsetzungsfähige Lösungen, sondern setzen im Dialog auch wesentliche Bedingungen, um den erfolgreichen Transfer von Forschungsergebnissen in die Praxis zu gewährleisten. Wichtige Impulse gehen auch von dem projektübergreifenden Dialog in den Innovationsplattformen aus. Unter dem Leitbild „Von der Forschung aus vorausdenken“ bieten sie allen Akteuren ein Forum, über Projektgrenzen hinweg Chancen eines erfolgreichen Innovationstransfers zu diskutieren. Darüber hinaus unterstützen wir mit der industriepolitischen Konzeption „Zukunftsmarkt zivile Sicherheit“ des Bundesministeriums für Wirtschaft und Technologie (BMWi) den Aufbau interdisziplinärer Netzwerke und regionaler Cluster.

Um die Vernetzung und Kommunikation zwischen den Projekten und Akteuren der zivilen Sicherheitsforschung zu verstetigen, planen wir, mit dem BMBF-Innovationsforum „Zivile Sicherheit“ eine nationale Konferenz zur zivilen Sicherheitsforschung zu etablieren. Hier werden in enger Kooperation der beteiligten Bundesministerien aktuelle Ergebnisse aus den Förderschwerpunkten vorgestellt und der Austausch zwischen Politik, Wissenschaft, Wirtschaft und Gesellschaft zu den zukünftigen Herausforderungen und grundlegenden Fragen der zivilen Sicherheit vorangetrieben.

Der Transfer von Wissen und Forschungsergebnissen in die Praxis erfordert eine gebündelte und umfassende Darstellung von Informationen und Forschungsaktivitäten. Deshalb wird das Internetportal www.sifo.de den Akteu-

ren der zivilen Sicherheitsforschung neue Kommunikations- und Interaktionsmöglichkeiten eröffnen.

Chancen durch Standardisierung

Der Transfer von Forschungsergebnissen in die Praxis kann durch die frühzeitige Einleitung von Standardisierungsprozessen unterstützt werden. Standardisierungen und Normungen können helfen, die internationale Vorreiterstellung deutscher Anbieter ziviler Sicherheitsprodukte und -technologien langfristig zu sichern bzw. auszubauen und gleichzeitig Anreize geben für die Beschaffung von innovativen Produkten. Neben kostenreduzierenden Effekten gewährleistet die Einführung europaweit einheitlicher Standards und Normen die Kompatibilität und Interoperabilität von Komponenten und Systemen.

Deshalb werden wir uns auf Grundlage des normungspolitischen Konzeptes der Bundesregierung aktiv dafür einsetzen, die Rolle der entwicklungsbegleitenden Standardisierung und Normung im Wachstumsfeld zivile Sicherheit weiter zu stärken. Die im November 2010 am Deutschen Institut für Normung (DIN) eingerichtete „Koordinierungsstelle Sicherheitswirtschaft“ soll den nationalen Normungs- und Standardisierungsbedarf identifizieren sowie den nationalen Meinungsbildungsprozess voranbringen und die rechtzeitige und koordinierte Einbringung nationaler Interessen auf europäischer und internationaler Ebene in der Normung fördern.

Das BMWi-Vorhaben „TNS – Transfer von FuE-Ergebnissen durch Normung und Standardisierung“ greift die Chancen der Normung für den beschleunigten Technologietransfer auf. Das technologieoffene, an Universitäten, Forschungseinrichtungen und innovative Unternehmen gerichtete Programm fördert gezielt Vorhaben an der Schnittstelle zwischen Forschung und Normung.

Validierung von Forschungsergebnissen und Zertifizierung

Eine transparente und unabhängige Validierung von Ergebnissen kann für den Endanwender Informationen über die Qualität, Interoperabilität und Leistungsfähigkeit von Sicherheitslösungen liefern. Diese Informationen schaffen Vergleichbarkeit und somit auch Investitionssicherheit (oder kalkulierbare Investitionsrisiken) für innovative Produkte.

Eine Grundlage für die Definition von Anforderungen können Normen und Standards sowie einheitliche Zertifizierungs- bzw. Konformitätsüberprüfungsverfahren für Sicherheitsprodukte, -systeme und -dienstleistungen bilden, indem sie die Anforderungen technologieneutral und konsensbasiert beschreiben. Die Verwendung von harmonisierten europäischen Normen trägt dabei zur Reduzierung der Marktfragmentierung bei. Damit ließen sich die Wettbewerbsbedingungen europäischer Unternehmen nicht nur in allen EU-Mitgliedstaaten deutlich verbessern, sondern es würden sich auch auf Drittmärkten Marktchancen eröffnen. Durch Einbringen europäischer Anforderungen in internationale Standards kann der weltweite Sicherheitsmarkt gestaltet werden. Mit einheitlichen Standards und Zertifizierungsverfahren, zum Beispiel durch ein EU-Security-Label, ließe sich zudem der bürokratische Aufwand verringern und dadurch Zeit und Kosten sparen, da ggf. erforderliche Mehrfachzertifizierungen entfielen.

Neue Impulse durch Beschaffung und Demonstrationsphasen

Auch wenn sich mittlerweile 80 Prozent der kritischen Infrastrukturen in privatwirtschaftlicher Hand befinden, ist der Staat im Bereich ziviler Sicherheit ein wichtiger Nachfrager von Innovationen.

Ausführliche Tests von Forschungsergebnissen in Demonstrationsphasen unter realen Einsatzbedingungen sowie die innovationsorientierte Beschaffung von Forschungsleistungen können einen wichtigen Impuls für den Transfer von Forschungsergebnissen in markt- bzw. beschaffungsfähige Produkte und Dienstleistungen geben. Durch innovationsorientierte Beschaffung kann ein Pioniermarkt geschaffen werden, der staatlichen wie privaten Endnutzern den Zugang zu innovativen Produkten und Dienstleistungen erleichtert.

Maßgeschneiderte Förderinstrumente

Gerade junge, dynamische Unternehmen mit einer starken Ausrichtung auf internationale Märkte, die Forschung im Hightech-Bereich betreiben, benötigen spezifische Unterstützung für ihre Forschungsvorhaben. Als Maßnahme der Hightech-Strategie zielt daher die Förderinitiative KMU-innovativ darauf ab, forschungsintensiven kleinen und mittleren Unternehmen einen erleichterten Zugang zu den Technologieförderprogrammen des BMBF zu ermöglichen. Hierzu trägt auch „KMU-innovativ: Forschung für die zivile Sicherheit“ bei.

Neben dem Rahmenprogramm Sicherheitsforschung gibt es auch technologieoffene F&E-Programme der Bundesregierung, die einen wesentlichen Beitrag zur Förderung der Sicherheitsforschung insbesondere für KMU leisten. Als Beispiele seien das Zentrale Innovationsprogramm Mittelstand (ZIM) oder die Industrielle Gemeinschaftsforschung (IGF) des BMWi genannt. Als zentrale Beratungsstelle informiert die Förderberatung „Forschung und Innovation“ des Bundes (www.foerderinfo.bund.de) über relevante Förderprogramme der Bundesministerien, der Bundesländer sowie der Europäischen Kommission.

Um den Transfer von Forschungsergebnissen in den Markt zu beschleunigen, ist es in der Endphase von Forschungsprojekten erforderlich, Projektpartnern, insbesondere den beteiligten KMU, Möglichkeiten der weitergehenden Unterstützung aufzuzeigen. Dazu werden wir verstärkt auf bestehende ressortübergreifende Beratungsinstrumente der Bundesregierung zurückgreifen. So bietet das Bundesministerium für Wirtschaft und Technologie BMWi im Rahmen seiner Technologieoffensive verschiedene Instrumente wie etwa Innovationsgutscheine (Go-Inno) an. Diese sind schwerpunktmäßig auf die technologieoffene Unterstützung innovativer KMU bei der Umsetzung von Innovationen ausgerichtet.

Um auch im Bereich der Sicherheitstechnik technologieorientierte und wissensbasierte Unternehmensgründungen gerade auch im Kontext der Hochschulen und außeruniversitären Forschungseinrichtungen in Deutschland zu unterstützen, bietet das BMWi das Förderprogramm „Existenzgründungen aus der Wissenschaft (EXIST)“ an. Flankierend können die Gründerteams Coachingleistungen in Anspruch nehmen. Daneben bietet das BMWi über den High-Tech-Gründerfonds neu gegründeten Technologieunternehmen eine erste Risikokapitalfinanzierung an und vermittelt ihnen das notwendige unternehmerische Know-how.

3.3 Wissenschaftliche Basis verbreitern und Kompetenzbildung unterstützen

Deutschland ist ein international anerkannter Wissenschafts- und Innovationsstandort, an dem nicht nur auf höchstem Niveau geforscht und gelehrt wird, sondern auch hochqualifizierte Fach- und Arbeitskräfte ausgebildet werden. Innovationspolitik, die sich den Herausforderungen des globalen Wettbewerbs stellt, muss dem langfristigen Bedarf an wissenschaftlich und technisch ausgebildeten Fachkräften eine hohe Priorität beimessen und Bildung und Ausbildung mit geeigneten Instrumenten fördern.

Gerade in der zivilen Sicherheitsforschung, in der Natur-, Ingenieur- und Gesellschaftswissenschaftlerinnen und -wissenschaftler verschiedenster Fachrichtungen gemeinsam innovative Lösungen entwikkeln, hat die Förderung und Qualifizierung des wissenschaftlichen Nachwuchses eine herausragende Bedeutung. Die Zahl der in diesem Bereich aktiven Forschungseinrichtungen und Hochschulen steigt stetig. Häufig ist die akademische Ausbildung auf die jeweilige Spezialdisziplin fokussiert. Es fehlt oftmals eine ausreichende Vernetzung zwischen den Fachgebieten und eine ausreichende Praxisorientierung. Die interdisziplinäre und interinstitutionelle Zusammenarbeit ist aber eine wesentliche Voraussetzung für eine führende Position in der Sicherheitsforschung und im Wettbewerb um die besten Wissenschaftlerinnen und Wissenschaftler.

Wir werden innerhalb der bestehenden Forschungs-, Exzellenz- und Nachwuchsförderung der Bundesregierung die Entwicklung der zivilen Sicherheitsforschung als Forschungsdisziplin aktiv begleiten und grundlegende Beiträge zur Verbreiterung der wissenschaftlichen Basis, zum Beispiel zur Ausarbeitung eines systemischen Ansatzes oder zum Recht der zivilen Sicherheit, unterstützen. Darüber hinaus gilt es, die Weiterentwicklung interdisziplinärer akademischer Ausbildungsstrukturen und -angebote in der zivilen Sicherheitsforschung zu fördern.

Wir wollen damit einen Beitrag zur Erhöhung der Qualität von Forschung und Lehre in der zivilen Sicherheitsforschung in Deutschland leisten und Maßstäbe für die europäische Sicherheitsforschung setzen. Dazu soll der Förderung junger Wissenschaftlerinnen und Wissenschaftler und dem Auf- und Ausbau wissenschaftlicher Exzellenznetze besondere Aufmerksamkeit eingeräumt werden. Es sollen spezielle Förderinstrumente zur Nachwuchsförderung unterstützt werden, zum Beispiel im Rahmen von Summerschools, Graduiertenschulen oder Nachwuchsgruppen. Um die Zusammenarbeit zwischen Wissenschaft und Praxis zu intensivieren, unterstützen wir den nationalen und internationalen Austausch von Wissenschaftlerinnen und Wissenschaftlern zwischen Hochschulen, Forschungseinrichtungen und Unternehmen.

Der richtige Umgang mit Risiken und konkreten Gefahrensituationen erfordert umfangreiche Kompetenzen und die Fähigkeit, das erworbene Wissen schnell und effektiv einzusetzen. Das gilt sowohl für die technischen und organisatorischen Kompetenzen von Sicherheits- und Rettungskräften sowie Mitarbeiterinnen und Mitarbeiter von Unternehmen als auch für die individuelle Sicherheitskompetenz der Bürgerinnen und Bürger. Diese Kompetenzen sollten frühzeitig entwickelt werden. Sie müssen durch weiteres Lernen und Training im Berufsleben, in ehrenamtlichen Tätigkeiten oder in Alltagssituationen entsprechend der technischen und gesellschaftlichen Anforderungen erweitert werden. Adressatengerechte Aus- und Weiterbildungskonzepte sowie eine bessere Vernetzung bestehender Bildungseinrichtungen und Trainingszentren tragen dazu bei, das Risikobewusstsein und die Handlungskompetenz von Mitarbeiterinnen und Mitarbeitern öffentlicher Einrichtungen und Unternehmen zu verbessern.

3.4 Internationale Zusammenarbeit stärken

Die zukünftigen Herausforderungen der zivilen Sicherheit sind nicht an Grenzen gebunden, sie sind häufig globaler Natur. Um den Schutz der Bevölkerung und der kritischen Infrastrukturen langfristig zu gewährleisten, sind der Ausbau der europäischen Forschungszusammenarbeit, die Mitgestaltung der europäischen Sicherheitsarchitektur sowie die Initiierung und Fortführung internationaler Forschungsallianzen wichtige Ziele des Rahmenprogramms „Forschung für die zivile Sicherheit“.

Bereits im 7. Forschungsrahmenprogramm hat die Europäische Union ein eigenes Sicherheitsforschungsprogramm aufgelegt, das wichtige Grundsteine für die EU-Zusammenarbeit gelegt hat. Auch im nächsten europäischen Rahmenprogramm für Forschung und Innovation („Horizon 2020“) wird die zivile Sicherheitsforschung als wichtiger thematischer Schwerpunkt verankert sein.

Wir werden insbesondere darauf achten, dass die im europäischen Sicherheitsforschungsprogramm adressierten Forschungsthemen auf einen klaren europäischen Mehrwert zielen. Nur so kann eine klare Arbeitsteilung und Verzahnung mit nationalen Aktivitäten erreicht und gleichzeitig eine erfolgreiche Beteiligung deutscher Akteure in der europäischen Sicherheitsforschung sichergestellt werden.

Wir werden die erfolgreiche Partnerschaft mit Frankreich intensivieren und sind grundsätzlich offen für Kooperationen mit weiteren europäischen Staaten, die über eigenständige nationale Forschungsprogramme im Bereich der zivilen Sicherheit verfügen. Die Zusammenarbeit soll auf Basis koordinierter bzw. gegenseitig geöffneter Bekannt-

machungen erfolgen. Forschergruppen sowie Unternehmen und Endnutzer aus den jeweiligen Staaten sollen die Gelegenheit erhalten, gemeinsam innovative Lösungen zu grenzübergreifenden Fragen der zivilen Sicherheit, zum Beispiel im Katastrophenschutz oder Krisenmanagement, zu entwickeln. Mit dieser Form der bilateralen Forschungszusammenarbeit wird nicht nur das Ziel verfolgt, die Sicherheit Deutschlands und des jeweiligen Partnerlandes zu erhöhen, sondern auch ein Beitrag zur Mitgestaltung der europäischen Sicherheitsarchitektur geleistet. Die im Rahmen europäischer Kooperationsprojekte entwickelten bilateralen Forschungs- und Lösungsansätze werden wir in den europäischen Forschungsraum tragen und so die thematische Ausrichtung des europäischen Sicherheitsforschungsprogramms unterstützen.

Deutschland strebt auf dem Gebiet der zivilen Sicherheitsforschung eine aktive Rolle an, um die Entwicklung von Lösungsansätzen für globale Herausforderungen mitzugestalten. Dazu ist es notwendig, durch Forschungsallianzen mit starken internationalen Technologiepartnern und Wachstumsmärkten weltweit verfügbares Wissen und Know-how für das nationale Programm nutzbar zu machen. Wir wollen deshalb die bestehenden bilateralen Kooperationen mit den USA und Israel ausbauen. Darüber hinaus streben wir gezielte bilaterale Forschungskooperationen mit Staaten an, die sich zu wichtigen Wachstumsmärkten der zivilen Sicherheit entwickeln werden.

Um auf internationaler Ebene die Verbindung von Forschung und Innovation für eine optimale Umsetzung der Forschungsergebnisse zu fördern, unterstützen wir grenzübergreifende Initiativen, die zum Beispiel europäische oder internationale Standardisierungs- und Normungsprozesse anstoßen.

4 Programme verzahnen

Mit dem neuen Rahmenprogramm „Forschung für die zivile Sicherheit“ setzt die Bundesregierung unmittelbar die Impulse der „Hightech-Strategie 2020 für Deutschland“ um. Dort ist Sicherheit – neben Klima/Energie, Gesundheit/Ernährung, Mobilität und Kommunikation – eines von fünf Bedarfsfeldern, an denen sich die innovationspolitischen Aktivitäten der Bundesregierung orientieren.

4.1 Rahmenprogramme der Bundesregierung

Rahmenprogramm „Schlüsseltechnologien und Querschnittsmaßnahmen“

Ziel des Rahmenprogramms ist es, durch die Bündelung strategischer Ansätze und konkreter Aktivitäten zur Entwicklung hochinnovativer Technologien und Dienste die internationale Spitzenstellung Deutschlands in den Schlüsseltechnologien zu sichern und auszubauen. In Verbindung mit flankierenden Querschnittsmaßnahmen soll die Förderung von Schlüsseltechnologien und Diensten dazu beitragen, die Basis für die Entwicklung neuer Produkte, innovativer Dienstleistungen und Verfahren zu schaffen, die die Wirtschaft stärken und zugleich Beiträge zur Lösung gesellschaftlicher Herausforderungen leisten. Durch die Förderung wichtiger Schlüsseltechnologien ist das Rahmenprogramm damit auch richtungsweisend für die Entwicklung darauf aufbauender innovativer ziviler Sicherheitslösungen. Das Rahmenprogramm „Schlüsseltechnologien und Querschnittsmaßnahmen“ befindet sich zurzeit in Vorbereitung.

Forschung für nachhaltige Entwicklungen – Rahmenprogramm des BMBF

Seit 2010 unterstützt das BMBF mit dem Rahmenprogramm „Forschung für nachhaltige Entwicklungen“ innerhalb der Hightech-Strategie die Forschung in den Bereichen Klima, Energie und natürliche Ressourcen. Ziel ist es, die nationalen Klimaschutzziele zu erreichen sowie Konzepte für die Anpassung an den Klimawandel zu entwickeln und einen Beitrag zur nationalen Nachhaltigkeitsstrategie zu leisten. Insbesondere durch die Weiterentwicklung von Vorsorge- und Frühwarnsystemen schafft das Rahmenprogramm wichtige technische und wissenschaftliche Grundlagen, auf denen im Rahmenprogramm „Forschung für die zivile Sicherheit“ innovative Lösungen zum Schutz der Bevölkerung vor natürlichen bzw. klimabedingten Extremereignissen entwickelt werden können.

Nationale Forschungsstrategie BioÖkonomie 2030

Die „Nationale Forschungsstrategie BioÖkonomie“ ist Bestandteil der Hightech-Strategie und liefert für diese u. a. in den Bedarfsfeldern Energie/Klima sowie Gesundheit/Ernährung wichtige Impulse. Mit der 2010 gestarteten Forschungsstrategie sollen in fünf prioritären Handlungsfeldern Grundlagen für die Entwicklung einer wissensbasierten und international wettbewerbsfähigen Bioökonomie gelegt werden; dies sind: weltweite Ernährungssicherheit, nachhaltige Agrarproduktion, gesunde und sichere Lebensmittel, industrielle Nutzung nachwachsender Rohstoffe sowie Energieträger auf Basis von Biomasse. Es soll die Entwicklung ganzheitlicher, bio-basierter Innovationen gefördert werden, die ökologische, wirtschaftliche und gesellschaftliche Belange gleichermaßen berücksichtigen und im Sinne nachhaltiger Lösungen integrieren.

Auch der Bereich der Lebensmittel ist, wie beispielsweise der sogenannte „Dioxinskandal“ gezeigt hat, mit Fragen der Sicherheit konfrontiert. Hier ergänzt und unterstützt das Programm „Forschung für die zivile Sicherheit“ die Ziele der „Nationalen Forschungsstrategie BioÖkonomie 2030“ insbesondere im Aktionsfeld „Gesunde und sichere Lebensmittel produzieren“.

Rahmenprogramm Gesundheitsforschung der Bundesregierung

Mit dem 2010 verabschiedeten „Rahmenprogramm Gesundheitsforschung“ richtet die Bundesregierung die Gesundheitsforschung neu aus. Durch eine engere Verknüpfung der Kompetenzen, Disziplinen und Institutionen sollen Forschungsergebnisse in Zukunft schneller aus der Grundlagen- und der klinischen Forschung in die medizinische Versorgung und damit zu den Patienten gelangen.

Die auf aktuellen Erkenntnissen basierende medizinische Behandlung soll letztendlich die Lebensqualität der Menschen verbessern. Neben einer inhaltlichen Fokussierung auf die Erforschung von Volkskrankheiten vor allem in „Deutschen Zentren der Gesundheitsforschung“ stehen auch die individualisierte Medizin, Präventions- und Ernährungsforschung, Gesundheitswirtschaft, Versorgungsforschung sowie die Gesundheitsforschung im Mittelpunkt dieses Programms.

Die Forschungsaktivitäten des Rahmenprogramms Gesundheitsforschung werden auch grundsätzliches Wissen zu sicherheitsrelevanten Themen, wie etwa zur Infektiologie, zu Zoonosen und zu Vektoren generieren, auf das die Aktivitäten des Rahmenprogramms „Forschung für die zivile Sicherheit“ insbesondere beim Schutz vor Pandemien und neuen Infektionskrankheiten aufbauen können.

6. Energieforschungsprogramm der Bundesregierung

Die Bundesregierung legt die Grundlinien und Schwerpunkte ihrer Energieforschungspolitik sowie die zugehörigen Fördermechanismen in einem mehrjährigen Energieforschungsprogramm fest. Im Juli 2011 wurde das 6. Energieforschungsprogramm „Forschung für eine umweltschonende, zuverlässige und bezahlbare Energieversorgung“ verabschiedet. Das neue Programm bildet einen wichtigen Schritt bei der Umsetzung des Energiekonzepts vom 28. September 2010, mit dem die Bundesregierung den Weg in das Zeitalter der erneuerbaren Energien beschreiten und eine sichere, wirtschaftliche und umweltverträgliche Energieversorgung gewährleisten will. Das Energieforschungsprogramm setzt sich u. a. mit Fragestellungen auseinander, die die Anpassung der Stromnetze durch den verstärkten Ausbau der erneuerbaren Energien und die zunehmende Dezentralisierung des Stromangebots betreffen. Das macht den Einsatz von neuen Technologien erforderlich, um in Zukunft eine effiziente, zuverlässige und sichere Stromübertragung bzw. Stromverteilung gewährleisten zu können.

Verkehrsforschungsprogramm der Bundesregierung

Im 3. Verkehrsforschungsprogramm der Bundesregierung „Mobilität und Verkehrstechnologien“ wurde 2008 unter Federführung des BMWi von fünf Bundesressorts ein Handlungsrahmen für die Förderung von Forschung und Entwicklung in drei strategischen Schwerpunkten erarbeitet: „Intelligente Logistik“, „Mobilität im 21. Jahrhundert“ sowie „Intelligente Verkehrsinfrastruktur“. Neben neuen technischen Lösungen zum Güterumschlag, der Automatisierung von Transportprozessen und einem intelligenten Verkehrsmanagement gehören auch neue Ansätze zur Erhöhung der Sicherheit im Straßenverkehr zum Aufgabenspektrum des Programms. Flankierend dazu hat 2010 das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) mit dem „Aktionsplan Güterverkehr und Logistik“ ein strategisches Konzept und konkrete Maßnahmen für die künftige Ausrichtung des Güterverkehrs erarbeitet.

Strategie der Bundesregierung zur Internationalisierung von Wissenschaft und Forschung

2008 wurde die Strategie der Bundesregierung zur Internationalisierung von Wissenschaft und Forschung „Deutschlands Rolle in der globalen Wissensgesellschaft stärken“ beschlossen. Darin wird die Internationalisierung von Wissenschaft und Forschung ressortübergreifend strukturiert. Ziel ist es, durch Kooperationen das zunehmende internationale Wissenspotenzial für den Wissenschafts- bzw. Innovationsstandort Deutschland nutzbar zu machen sowie Deutschlands Rolle in der globalen Wissensgesellschaft zu stärken. Mit dem Rahmenprogramm Internationalisierung entwickelt das BMBF auf Grundlage dieser Internationalisierungsstrategie einen praxisrelevanten Orientierungsrahmen für alle internationalen BMBF-Aktivitäten in den Bereichen Forschung wie Bildung.

4.2 Ressortforschung und institutionelle Förderung

Die außeruniversitäre Wissenschaft trägt wesentlich dazu bei, die wissenschaftliche Basis in der zivilen Sicherheitsforschung zu verbreitern. Dabei spielen Forschungsorganisationen wie die Helmholtz-Gemeinschaft, die Fraunhofer-Gesellschaft, die Leibniz-Gemeinschaft und die Max-Planck-Gesellschaft sowie die Ressortforschungseinrichtungen des Bundes mit ihren unterschiedlichen Profilen und Schwerpunkten eine besondere Rolle. Die institutionelle Förderung und die Ressortforschung sollen eng mit dem Rahmenprogramm verzahnt werden. Vorrangiges Ziel ist es, die Arbeitsteilung, Schwerpunktbildung und Vernetzung in der zivilen Sicherheitsforschung zu optimieren.

Ressortforschung

Die Bundesregierung kann sich in der zivilen Sicherheitsforschung auf eine breit gefächerte Ressortforschung stützen.

Als Ressorteinrichtungen mit Bezug zur zivilen Sicherheitsforschung sind im Geschäftsbereich des BMI besonders zu erwähnen: das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), die Bundesanstalt Technisches Hilfswerk (THW), das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Bundeskriminalamt sowie die Bundespolizei mit der Forschungs- und Erprobungsstelle in Lübeck. Die genannten Einrichtungen verfolgen unter anderem das Ziel, wissenschaftliche Erkenntnisse für die Wahrnehmung von hoheitlichen bzw. fachlichen Aufgaben mit Schwerpunkt in den Bereichen Bevölkerungsschutz, IT-Grundschutz und Cybersicherheit, Schutz kritischer Infrastrukturen, Bekämpfung der Kriminalität (z. B. Terrorismus, organisierte Kriminalität und Gewaltkriminalität) sowie Grenzschutz und Luftsicherheit zu gewinnen.

Im Geschäftsbereich des BMWi ist die Bundesanstalt für Materialforschung und -prüfung (BAM) zu nennen, die als wissenschaftlich-technische Bundesoberbehörde Forschungsexpertisen in der technischen Sicherheit u. a. im

Bereich des sicheren Umgangs mit Gefahrstoffen und Gefahrgütern sowie zu neuen Analyse- und Prüftechniken aufweist. Die Physikalisch-Technische Bundesanstalt (PTB) betreibt Grundlagenforschung und Entwicklung im Bereich der Metrologie als Basis für alle ihre Aufgaben, unter anderem in den Bereichen Sicherheitstechnik, Dienstleistung und Messtechnik für den gesetzlich geregelten Bereich und die Industrie sowie für den Technologie-Transfer. Durch die Sicherstellung der Rückführbarkeit von Messungen, z. B. bei Kontrollen oder im Schadensfall bei der Spurensicherung, werden die Messergebnisse gerichtsfest.

Als Ressortforschungseinrichtung des BMVBS leistet die Bundesanstalt für Straßenwesen (BASt) eigene Forschungsarbeit; unter anderem zur Verbesserung der Erhaltung von Straßen, Brücken und Ingenieurbauwerken sowie zur Verbesserung der Verkehrssicherheit.

Forschungseinrichtungen des Bundesministeriums für Gesundheit (BMG) mit Bezug zur zivilen Sicherheit sind das Paul-Ehrlich-Institut (PEI) mit Forschungsschwerpunkten im Bereich der Impfstoffvorsorge und der Sicherheit biomedizinischer Arzneimittel sowie das Robert Koch-Institut (RKI), das als zentrale Referenzeinrichtung des Bundes für den öffentlichen Gesundheitsdienst unter anderem anwendungs- und maßnahmenorientierte Forschung zur Erkennung, Verhütung und Bekämpfung von Krankheiten sowie zur Erhebung und Aufbereitung von Gesundheitsdaten betreibt.

Das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV) hat ebenfalls eine Anzahl nachgeordneter Behörden und Forschungseinrichtungen, die Schwerpunkte in der zivilen Sicherheitsforschung aufweisen. Dazu zählen insbesondere das Friedrich-Loeffler-Institut (FLI) mit Forschungsarbeiten unter anderem zu Präventionsmaßnahmen sowie der Diagnose und Bekämpfung von Tierseuchen und Zoonosen sowie das Bundesinstitut für Risikobewertung (BfR), das unter anderem Forschung zur Lebensmittelsicherheit, zum gesundheitlichen Verbraucherschutz sowie zur Risikobewertung im Rahmen biologischer Sicherheit betreibt. Weitere Einrichtungen sind das Bundesamt für Verbraucherschutz und Lebensmittelsicherheit (BVL), das Max Rubner-Institut (MRI) – Bundesforschungsinstitut für Ernährung und Lebensmittel sowie das Julius Kühnen-Institut (JKI) – Bundesforschungsinstitut für Kulturpflanzen.

Das dem Geschäftsbereich des BMBF zugeordnete Bundesinstitut für Berufsbildung (BIBB) ist das Kompetenzzentrum zur Erforschung und Weiterentwicklung der beruflichen Aus- und Weiterbildung in Deutschland. Das BIBB identifiziert Zukunftsaufgaben der Berufsbildung, fördert Innovationen in der nationalen wie internationalen Berufsbildung und entwickelt neue, praxisorientierte Lösungsvorschläge für die berufliche Aus- und Weiterbildung, unter anderem auch im Bereich der sicherheitsrelevanten Berufe.

Institutionelle Förderung

Im Bereich der institutionellen außeruniversitären Förderung gibt es insbesondere bei den vier großen Forschungsorganisationen Fraunhofer-Gesellschaft (FhG), Helmholtz-Gemeinschaft (HGF), Leibniz-Gemeinschaft (WGL) und Max-Planck-Gesellschaft (MPG) zunehmend Bestrebungen, die zivile Sicherheit als eigenständigen Forschungsschwerpunkt aufzugreifen. Im Rahmen von Forschungskooperationen sowie in zahlreichen Forschungseinrichtungen und interdisziplinären Arbeitsgruppen werden vielfältige grundlagen- und anwendungsorientierte Ansätze verfolgt, die einen wichtigen Beitrag zur Weiterentwicklung der zivilen Sicherheitsforschung leisten.

Die Fraunhofer-Gesellschaft koordiniert zum Beispiel ihre Forschungsaktivitäten im Bereich der zivilen und verteidigungsbezogenen Sicherheitsforschung vor allem in dem 2002 gegründeten Fraunhofer-Verbund „Verteidigungs- und Sicherheitsforschung“ (VVS). In seinen derzeit zehn Mitgliedsinstituten schafft der Verbund durch die Bündelung seiner ingenieur- und naturwissenschaftlichen Kompetenzen wichtige Voraussetzungen, um die zukünftige Entwicklung system- und technologieorientierter Innovationen für die zivile Sicherheit voranzutreiben.

Auch in der Helmholtz-Gemeinschaft, der größten Wissenschaftsorganisation Deutschlands, wird die verfügbare Expertise im Bereich der zivilen Sicherheit in eigenen Forschungsschwerpunkten sowie durch die Bildung von zentrenübergreifenden Forschungseinrichtungen zusammengeführt. So plant und steuert das Deutsche Zentrum für Luft- und Raumfahrt (DLR) in einem Themenschwerpunkt Sicherheit seine Forschungs- und Entwicklungsaktivitäten mit verteidigungs- und sicherheitsrelevantem Bezug in Abstimmung mit den Partnern von Staat, Wissenschaft und Industrie. Ein weiteres Beispiel ist das „Center for Disaster Management and Risk Reduction Technology“ (CEDIM), eine interdisziplinäre Forschungseinrichtung des Helmholtz-Zentrums Potsdam Deutsches Geoforschungszentrum (GFZ) und des Karlsruher Instituts für Technologie (KIT) im Bereich des Katastrophenmanagements. Hier arbeiten derzeit Wissenschaftlerinnen und Wissenschaftler aus mehr als 15 Instituten unter anderem daran, zukünftig natürliche und anthropogene Risiken besser zu verstehen, früher zu erkennen und die Folgen von Katastrophen besser zu beherrschen.

5 Glossar

Ad-hoc-Kommunikationssysteme: Mobile, drahtlose Kommunikationssysteme, die sich zu selbst organisierenden und konfigurierenden Netzwerken verbinden können.

Behörden und Organisationen mit Sicherheitsaufgaben (BOS): Bezeichnung für staatliche und nicht-staatliche Akteure, die Aufgaben der inneren Gefahrenabwehr übernehmen wie zum Beispiel Polizei, Zoll, gemeinnützige Vereine oder private Hilfsorganisationen und Unternehmen mit Bezug zum Bevölkerungsschutz.

Bevölkerungsschutz: Oberbegriff für alle nicht-polizeilichen Aufgaben und Maßnahmen der Kommunen und der Länder im Katastrophenschutz sowie des Bundes im Zivilschutz.

Cyberraum: Der Cyberraum ist der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab.

Cybersicherheit: Cybersicherheit ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des Cyberraums auf ein tragbares Maß reduziert sind.

Dunkelfeld: Aus der Kriminalistik stammender Begriff, der die Differenz zwischen amtlich registrierten Straftaten und den tatsächlich begangenen, aber nicht erfassten Straftaten bezeichnet.

e-Government: Unter e-Government (oder „electronic Government") versteht man die Nutzung elektronischer Informations- und Kommunikationstechnik für die Durchführung von Prozessen zwischen staatlichen Institutionen untereinander und gegenüber Bürgern bzw. der Zivilgesellschaft.

Epidemie: Eine Epidemie ist ein zeitlich und räumlich begrenztes massenhaftes Auftreten einer Krankheit innerhalb einer Population.

Erweiterter Sicherheitsbegriff: Bezeichnet ein Verständnis von Sicherheit, das über die klassische Definition der militärischen Sicherheit hinausgeht und im Zuge der Globalisierung auch zivile Aspekte von Sicherheit einschließt, unter anderem kulturelle, soziale, ökologische und ökonomische.

Feldprogrammierbares Gate Array (FPGA): Bezeichnung eines integrierten Schaltkreises (IC) der Digitaltechnik, der nach dem Herstellungsprozess hardwareseitig programmiert und jederzeit aktualisiert, beziehungsweise vollständig neu konfiguriert werden kann.

Geomagnetische Stürme: Störung der Magnetosphäre der Erde, ausgelöst durch Schockwellenfronten starker Sonneneruptionen, durch die sich das Erdmagnetfeld verändert.

Honeynet: Ein (Computer-)Netzwerk, in das absichtlich Sicherheitslücken eingebaut sind mit dem Ziel, potenzielle Hacker zu ködern.

Informationeller Angriff: Bezeichnet wie der synonyme Begriff „Cyberangriff" einen im Cyberraum durchgeführten IT-Angriff, der sich gegen ein oder mehrere andere IT-Systeme richtet und zum Ziel hat, die IT-Sicherheit zu brechen und widerrechtlich Informationen einer anderen Person oder Institution auszuwerten, zu verfälschen oder IT-Infrastrukturen zu sabotieren bzw. zu zerstören.

Informationelle Selbstbestimmung: Ausdruck für das Grundrecht jeder Person, selbst über die Preisgabe und Verwendung von eigenen, personenbezogenen Daten zu entscheiden.

Interdependenzen: Allgemeine Bezeichnung von wechselseitigen Abhängigkeiten, z. B. im Sinne der wechselseitigen Abhängigkeit von kritischen Infrastrukturen, bei denen der Ausfall einer Komponente zu weiteren Ausfällen anderer Komponenten führen kann.

Internet der Dinge: Zukunftstechnologie, die es ermöglicht, dass sich alltägliche Gegenstände, Produkte, Maschinen oder Räume über das Internet vernetzen, Informationen austauschen und mit ihrer Umgebung interagieren können.

IT-Grundschutz: Ein auf nationaler Ebene etablierter Katalog von Standardsicherheitsmaßnahmen zur Risikominimierung für den Betrieb von Informationstechnik.

Kritische Infrastrukturen: Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Kryptoverfahren: Verfahren der IT-Sicherheit, bei dem Daten, Informationen oder Kommunikation mithilfe mathematischer Verfahren bzw. Transformationen verschlüsselt werden.

Massenanfall von Verletzten (MANV): Ein Massenanfall von Verletzten ist ein Notfall mit einer größeren Anzahl von Verletzten oder Erkrankten sowie anderen Geschädigten oder Betroffenen, der mit der vorhandenen und einsetzbaren Vorhaltung des Rettungsdienstes aus dem Rettungsdienstbereich nicht bewältigt werden kann.

Metrologie: Metrologie ist die Lehre von Maßen und Maßsystemen und wird in erweiterter Form auch als Synonym für „Wissenschaft und Technik des Messens" verwendet, die sich mit der Erfassung, Verarbeitung, Darstellung und Weitergabe von Informationen aus beliebigen Prozessen beschäftigt.

Pandemie: Die Pandemie ist im Gegensatz zur Epidemie ein länder- bzw. kontinentübergreifendes massenhaftes Auftreten einer Erkrankung.

Privacy by design: Das Konzept „Privacy by design" (oder eingebauter Datenschutz) zielt darauf ab, den Schutz der Privatsphäre und den Datenschutz von Anfang an in die Spezifikationen und die Architektur von Informations- und Kommunikationssystemen und -technologien zu integrieren.

Resilienz: Ursprünglich aus der Kybernetik stammender Begriff, der die Toleranz oder Widerstandsfähigkeit eines Systems vor störenden äußeren Einflüssen beschreibt.

RFID-Transponder: Die Abkürzung RFID entstammt dem englischen Begriff „Radio Frequency Identification" und bedeutet Funkerkennung. Transponder ist ein Kunstwort und setzt sich aus den Begriffen „Transmitter" und „Responder" zusammen (andere gängige Bezeichnungen sind u. a. RFID-Etiketten, RFID-Tags oder RFID-Label). Mithilfe von RFID-Transpondern können gespeicherte Daten berührungslos und ohne Sichtkontakt über Funk gelesen bzw. gespeichert werden.

SARS: Abkürzung für „Severe Acute Respiratory Syndrome". Eine Infektionskrankheit, die zu schweren Atem-

beschwerden führt sowie zu hohem Fieber, Husten und Halsschmerzen und in schweren Fällen einen lebensbedrohlichen Verlauf nehmen kann.

Security by design: Security by Design (Sicherheit als Designkriterium) bezeichnet den konzeptionsintegrierten Ansatz, Sicherheitsanforderungen frühzeitig als Planungsgrundlage bei der Entwicklung z. B. von Produkten, IT-Anwendungen oder Geschäftsmodellen einzubeziehen.

Seitenkanalangriffe: Seitenkanalangriffe stellen eine besondere Form eines Hackerangriffs dar, bei der versucht wird, über das Messen physikalischer Größen (wie z. B. der Abstrahlung, des Versorgungsstroms) an einem Gerät Rückschlüsse auf geheime Informationen zu gewinnen.

Sicherheitskultur: Gesamtheit der Überzeugungen, Werte und Praktiken von Individuen und Organisationen, die darüber entscheiden, was als eine Gefahr anzusehen ist und mit welchen Mitteln ihr begegnet werden soll.

Smart Grid: Der Begriff „Smart Grid" (Intelligentes Energieversorgungssystem) umfasst die Vernetzung und Steuerung von intelligenten Erzeugern, Speichern, Verbrauchern und Netzbetriebsmitteln in Energieübertragungs- und -verteilungsnetzen mithilfe von Informations- und Kommunikationstechnik.

Social Media: Digitale Medien, die es ermöglichen, sich interaktiv mit anderen auszutauschen. Als Kommunikationsmittel dienen dabei Text, Bild, Audio und/oder Video.

Telemedizinische Anwendungen: Anwendungen zur Diagnostik und Therapie von Krankheiten mittels Telekommunikation.

Toxine: Unter Toxinen (vom griechischen *toxíne* – die giftige Substanz) versteht man von Mikroorganismen, Pflanzen oder Tieren produzierte giftige Substanzen, die Organismen schädigen, indem sie die physiologischen Stoffwechselabläufe stören.

Triagierung: Ein in der Katastrophenmedizin gebräuchlicher Begriff (französisch vom Verb „trier" = sortieren, hergeleitet) zur Entscheidung über die Weiterbehandlung bzw. Behandlungspriorität von verletzten Personen bei knappen personellen und materiellen Ressourcen.

Trusted Computing: Der Begriff bedeutet „vertrauenswürdige Datenverarbeitung" und umschreibt neue Ansätze zur Verbesserung der Computersicherheit durch vertrauenswürdige Hardware- und Softwarekomponenten.

Vektoren: Der Begriff Vektor (lat. *vector* „jemand, der trägt, zieht oder befördert") bezeichnet in der Biologie und der Medizin ganz allgemein einen Überträger (z. B. Insekt) von Infektionskrankheiten auslösenden Krankheitserregern.

Zoonosen: Zoonosen (von griechisch *zoon* „Lebewesen" und *nosos* „Krankheit") sind von Tier zu Mensch und von Mensch zu Tier übertragbare Infektionskrankheiten.



Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333